ZYXEL
NETWORKS

User's Guide

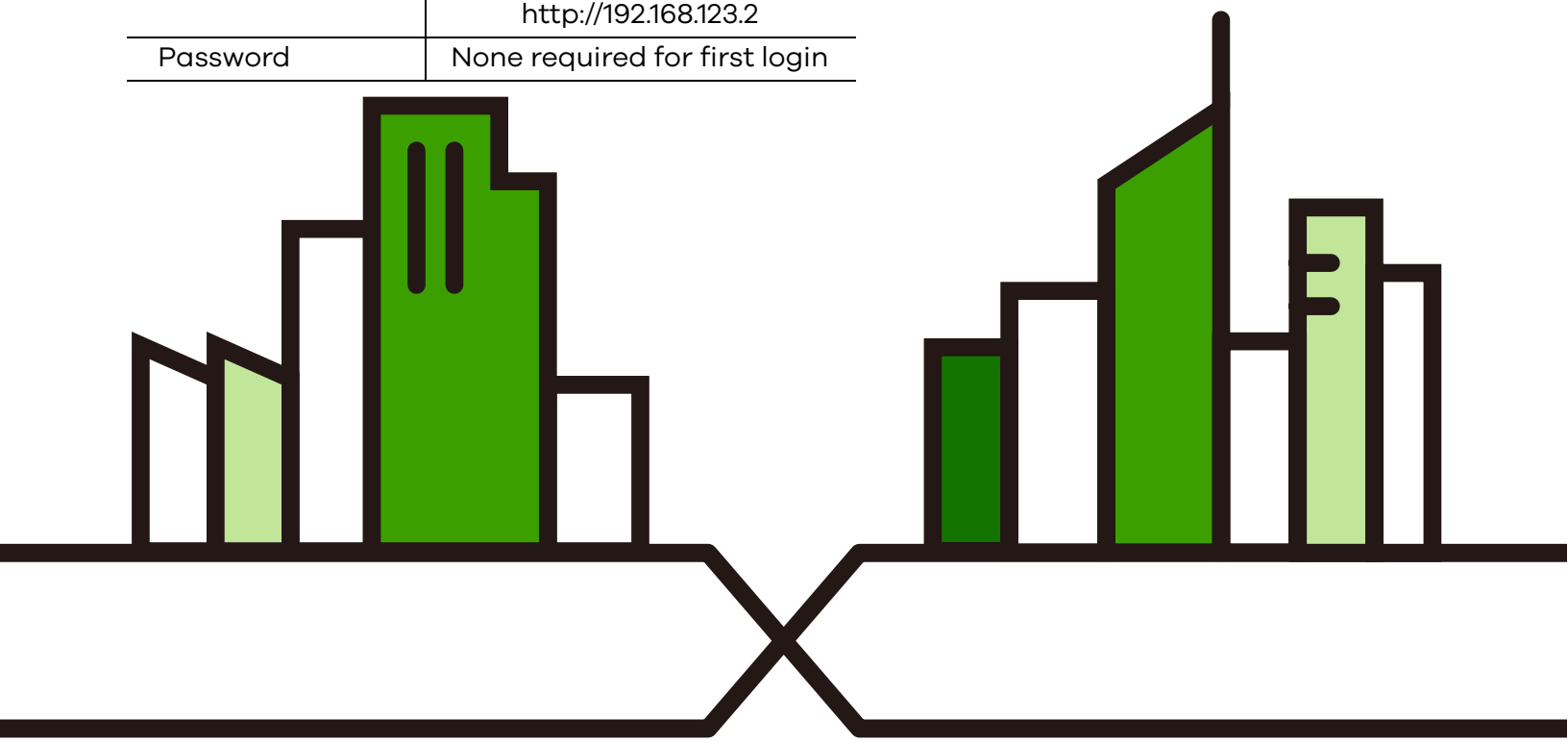
ARMOR G1

AC2600 Multi-Gigabit Security WiFi Router
Model: NBG6818

Default Login Details

LAN IP Address Standard (Router) Mode	http://zyxelwifi.com OR http://zyxelwifi.net OR http://192.168.123.1
Bridge Mode	http://DHCP-assigned IP OR http://192.168.123.2
Password	None required for first login

Version 1.00 Edition 4, 5/2022



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the NBG6818 and access the Web Configurator wizards. It contains information on setting up your network and configuring for Internet access.

- More Information

  Go to support.zyxel.com to find other information on the NBG6818.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Settings > Internet > Internet Connection** means you first click **Settings** in the navigation panel, then the **Internet** sub menu and finally the **Internet Connection** tab to get to that screen.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The NBG6818 icon is not an exact representation of your device.

NBG6818 	Wireless Device 	Laptop Computer 
Switch 	Firewall 	Server 
Internet 	Desktop Computer 	Smartphone 

Contents Overview

Table of Contents

PART I
User's Guide

CHAPTER 1
Introduction

1.1 NBG6818 Overview

This chapter introduces the main features and applications of the NBG6818, also called ARMOR G1.

The NBG6818 is able to work on both 2.4G and 5G networks. It supports OpenVPN (server and client), firewall for IPv4 and IPv6, and multi-gigabit port.

This table summarizes some of the features that are available at the time of writing.

Table 1 Features Supported on the NBG6818

FEATURES	NBG6818
Number of 2.5G/1G WAN port	1
Number of 1 Gbps Ethernet LAN ports	4
Number of USB port	1
Rubber feet for desktop placement	Yes
Wall-mount	Yes
Operating mode	Router and Bridge
Mobile app	ARMOR
OpenVPN (Server and Client)	Yes (router mode)
WiFi network	IEEE 802.11a/b/g/n/ac compatible
Guest WiFi	Yes (router mode)
Firewall (IPv4 and IPv6)	Yes
NAT and Port Forwarding	Yes (router mode)
ALG (Application Layer Gateway)	Yes (router mode)
VPN (Virtual Private Network) Pass-through	Yes (router mode)
Port Triggering	Yes (router mode)
Dynamic DNS (Domain Name System)	Yes (router mode)
Parental Control	Yes (router mode)
IPv6 support	Yes (router mode)
UPnP (Universal Plug-and-Play)	Yes (router mode)
USB for file sharing (Samba)	Yes
USB file sharing using FTP	Yes
USB media sharing	Yes
Save configuration	Yes

1.2 Applications for the NBG6818

The NBG6818 supports the following applications.

Multi-Gigabit

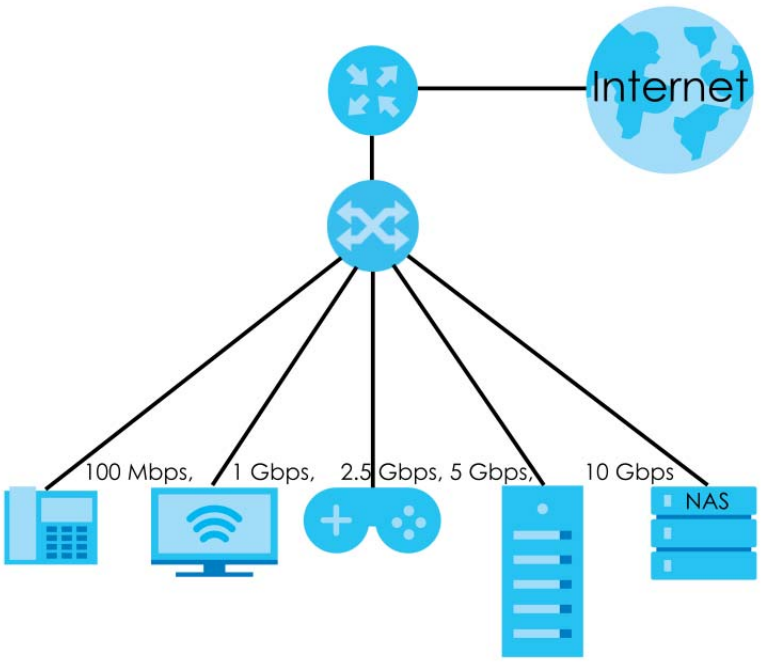
A 10 Gigabit port supports speed of 10 Gbps if the connected device supports 10 Gbps and a Cat 6a (up to 100 m) or Cat 6 cable (up to 50 m) is used. The speed drops to 1G if these criteria are not met; it drops to 100 Mbps if a Cat 5 cable is used (up to 100 m).

If a network device such as a 5G network card, gaming computer, server, Network Attached Storage (NAS) or Access Point (AP) only supports 2.5 Gigabit or 5 Gigabit connectivity, then the maximum speed potential of these devices is never reached.

In addition, at the time of writing, most existing cabling is Cat 5e or Cat 6, further limiting maximum speed or distance potential.

Multi-Gigabit (IEEE 802.3bz) solves these problems by additionally supporting 2.5 Gigabit and 5 Gigabit Ethernet connections over Cat 5e and higher Ethernet cables. Multi-Gigabit ports are also backward compatible with 100 Mbps and 1 Gigabit ports.

Figure 1 Multi-Gigabit Application



See the following table for the cables required and distance limitation to attain the corresponding speed.

Table 2 Ethernet Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100 Mbps	100 m	100 MHz
Category 5e	1 Gbps / 2.5 Gbps / 5 Gbps	100 m	100 MHz
Category 6	5 Gbps / 10 Gbps	50 m	250 MHz

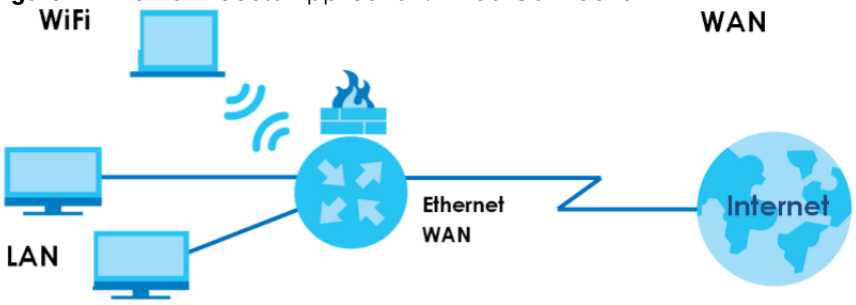
Table 2 Ethernet Cable Types (continued)

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 6a	10 Gbps	100 m	500 MHz
Category 7	10 Gbps	100 m	650 MHz

Internet Access

Your NBG6818 provides shared Internet access by connecting an Ethernet cable provided by the ISP (Internet Service Provider) to the **2.5G/1G** port. Connect network devices through the Ethernet ports of the NBG6818 (or wirelessly) so that they can communicate with each other and access the Internet.

Figure 2 Internet Access Application: Wired Connection

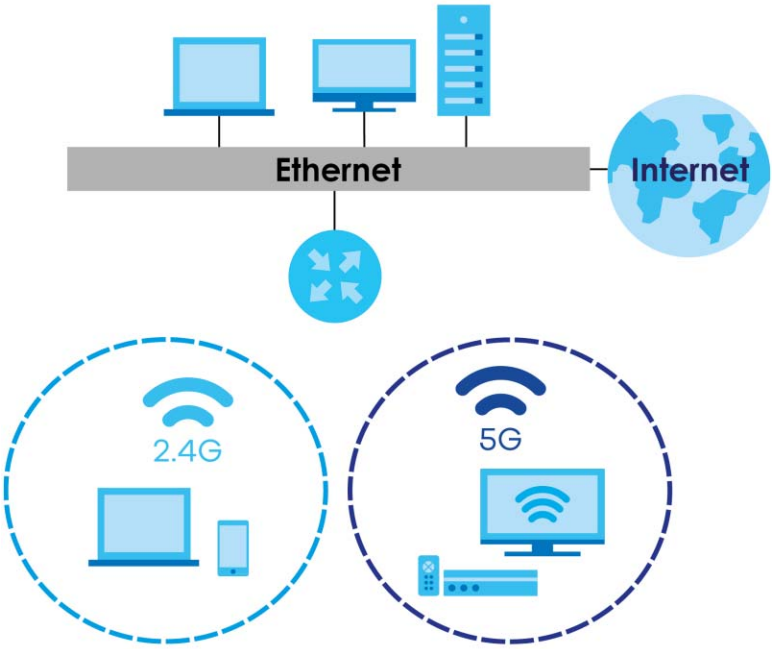


Dual-Band WiFi

IEEE 802.11a/b/g/n/ac compliant clients can wirelessly connect to the NBG6818 to access network resources.

The NBG6818 is a dual-band gateway that can use both 2.4G and 5G networks at the same time. You can use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

Figure 3 Dual-Band Application



You can use WPS (WiFi Protected Setup) to create an instant WiFi network connection with another WPS-compatible device.

Guest WiFi

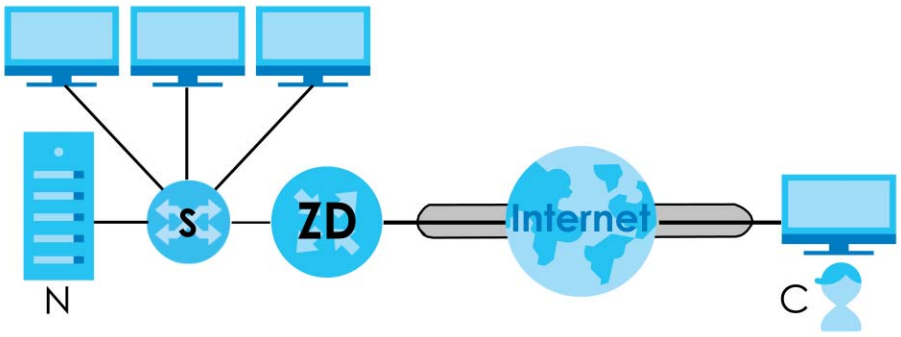
The NBG6818 allows you to set up a guest WiFi network where users can access the Internet through NBG6818, but not to other networks connected to it.

OpenVPN Server/Client

Your NBG6818 supports OpenVPN. OpenVPN is a VPN protocol which is open source and free of charge. It can be used to create a virtual private network or to interconnect local networks. It uses OpenSSL encryption library and SSLv3/TLSv1 protocols. This provides high security and anonymity for all transmitted data. It also provides faster connection speeds than other VPN protocols.

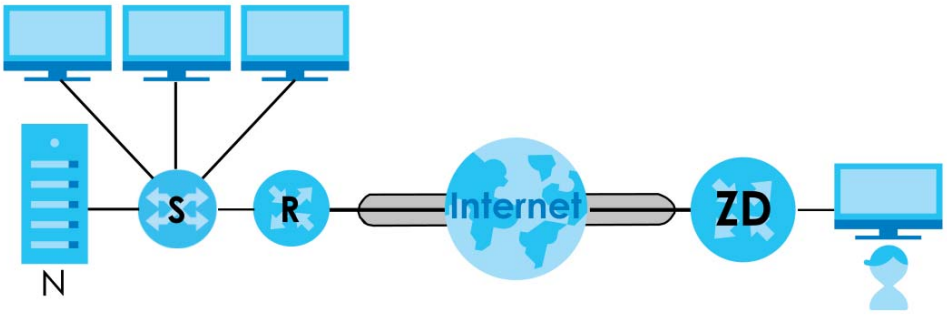
The following figure illustrates the NBG6818 (**ZD**) connected to a server network (**N**) through an Ethernet switch (S) function as an OpenVPN Server that transmit data to a client device (**C**) through a secure VPN channel.

Figure 4 OpenVPN Server Application



Alternatively, the following figure illustrates the NBG6818 (**ZD**) function as an OpenVPN Client to allow a VPN server (**R**) connected to a server network (**N**) through an Ethernet switch (**S**) to transmit data through a secure VPN channel to a client device connected to the NBG6818 (**ZD**).

Figure 5 OpenVPN Client Application



IPv6 and IPv6 Firewall

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses. The NBG6818 can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and support IPv6 rapid deployment (6RD).

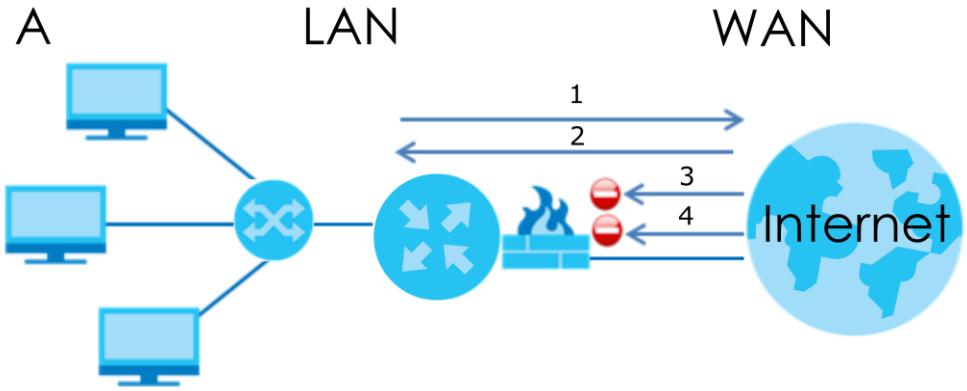
Consequently, you can enable and create IPv6 firewall rules to filter IPv6 traffic.

Firewall protects your NBG6818 and network from attacks by hackers on the Internet and control access to it. The firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (**1**). Return traffic for this session is also allowed (**2**). However other traffic initiated from the WAN is blocked (**3** and **4**).

Figure 6 Default Firewall Action

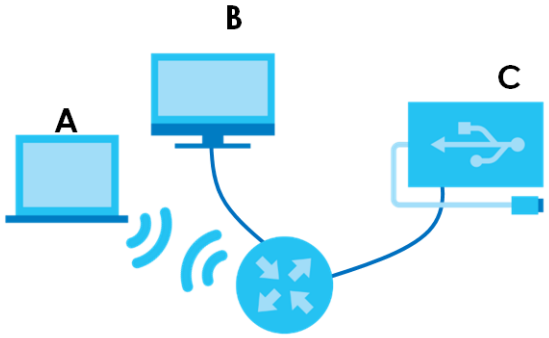


USB File Sharing

Share files on a USB memory stick or hard drive connected to your NBG6818 with users on your network. The NBG6818 also supports file sharing using FTP (file transfer protocol).

The following figure illustrates the NBG6818's file server feature. Computers (**A**) and (**B**) can access files on a USB device (**C**) which is connected to the NBG6818.

Figure 7 File Sharing Overview



USB Media Sharing

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your NBG6818 without having to copy them to another computer. The NBG6818 can function as a DLNA-compliant media server, where the NBG6818 streams files to DLNA-compliant media clients like Windows Media Player.

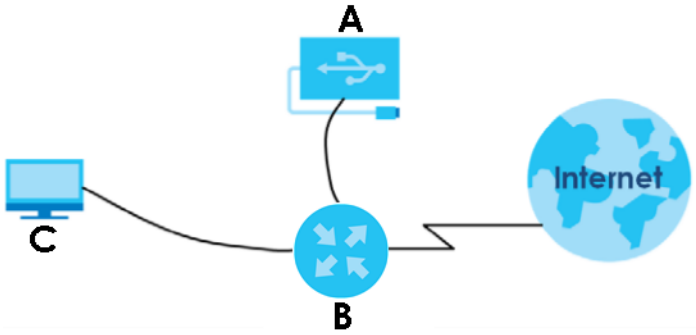
The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

The NBG6818 media server enables you to:

- Publish all share folders for everyone to play media files in the USB storage device connected to the NBG6818.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published folders. No user name and password nor other form of security is required.

Figure 8 Media Server Overview



The figure above illustrates a USB storage device (**A**) containing media files connected to the NBG6818 (**B**). A computer (**C**) with Windows Media Player installed can play the files.

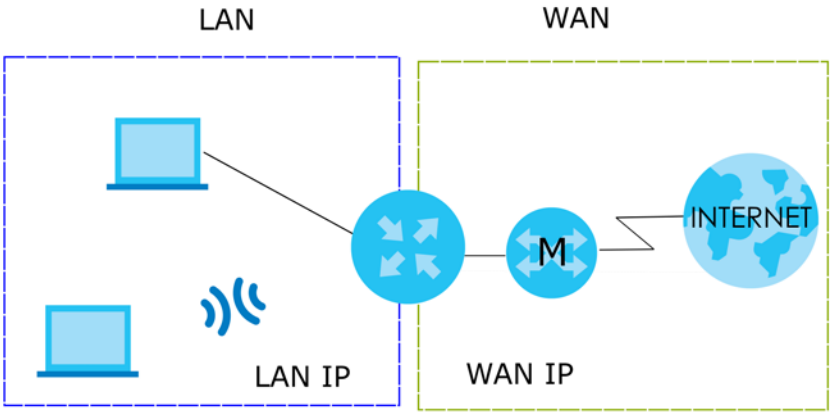
1.3 Operating Modes for the NBG6818

The NBG6818 is available in both Standard (router) mode and bridge mode.

1.3.1 Standard (Router) Mode

The NBG6818 is set to standard (router) mode by default. The NBG6818 is used to connect the local network to another network (for example, the Internet). In standard mode NBG6818 has two IP addresses, a LAN IP address and a WAN IP address. It also has more routing features. In the example scenario below, NBG6818 connects the local network to the Internet through a modem (**M**).

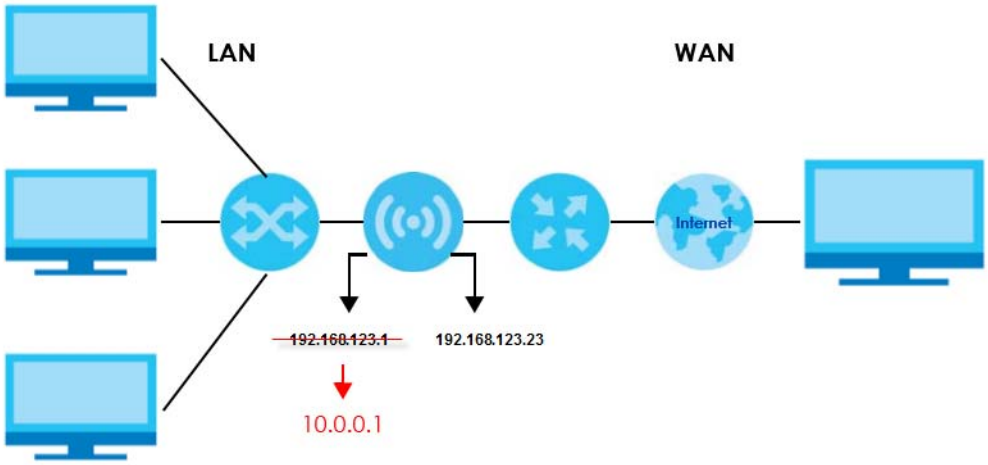
Figure 9 Standard Mode Example



Auto-IP Change

When the NBG6818 (**A**) gets a WAN IP address or a DNS server IP address which is in the same subnet as the LAN IP address 192.168.123.1, Auto-IP Change allows the NBG6818 to change its LAN IP address to 10.0.0.1 automatically. If the NBG6818's original LAN IP address is 10.0.0.1 and the WAN IP address is in the same subnet, such as 10.0.0.3, the NBG6818 switches to use 192.168.123.1 as its LAN IP address.

Figure 10 Auto-IP Change Example



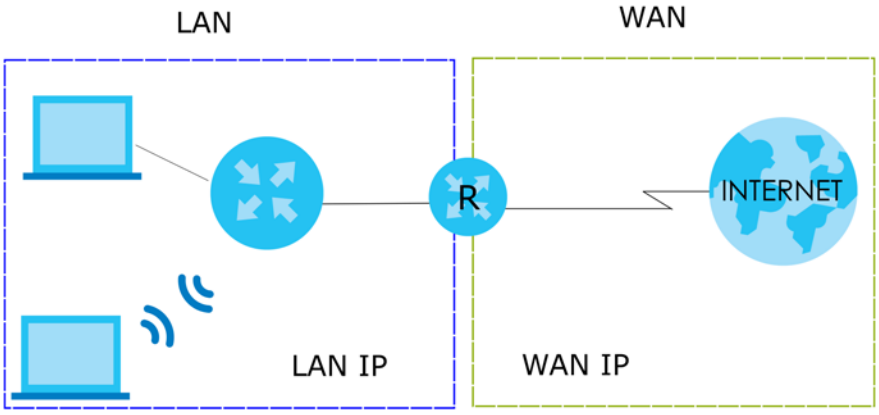
Auto-IP Change only works under the following conditions:

- The NBG6818 must be in standard (router) mode for Auto-IP Change to become active.
- The NBG6818 is set to receive a dynamic WAN IP address.

1.3.2 Bridge Mode

Use your NBG6818 as a bridge if you already have a router or gateway on your network. In this mode your NBG6818 bridges a wired network (LAN) and WiFi in the same subnet. In bridge mode, NBG6818 has one IP address and NBG6818 interfaces are bridged together in the same network. In the example scenario below, NBG6818 connects the local network to the Internet through a router (**R**).

Figure 11 Bridge Mode Example



1.4 Ways to Manage the NBG6818

Use the following method to manage the NBG6818.

- Web Configurator. This is recommended for everyday management of the NBG6818 using a (supported) web browser.

- [Company Name] ARMOR mobile app. This is the app you can use to manage the NBG6818 on your cellphone. To install the app, scan the QR code on the QSG.

1.5 Good Habits for Managing the NBG6818

Do the following things regularly to make the NBG6818 more secure and to manage the NBG6818 more effectively.

- Change the password. Use a password that is not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.

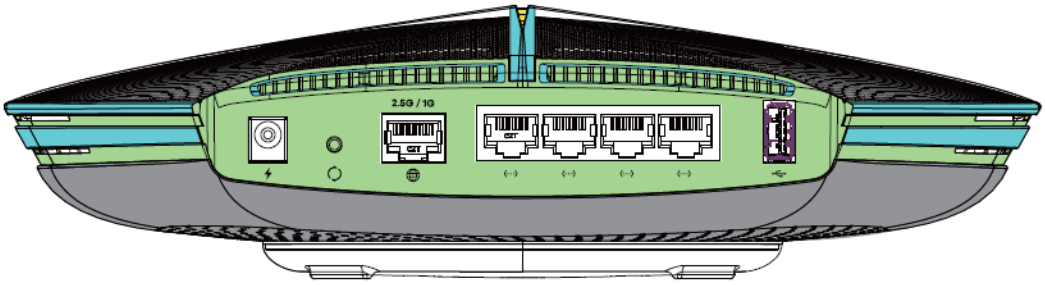
CHAPTER 2
Hardware

This chapter describes the front panel LED and rear panel of the NBG6818 and shows you how to mount the NBG6818 on the desk or wall.

2.1 Rear Panel

The following figure show the rear panel of the NBG6818. The rear panel contains:

Figure 12 Rear Panel Ports



The following table describes the items on the rear panel.

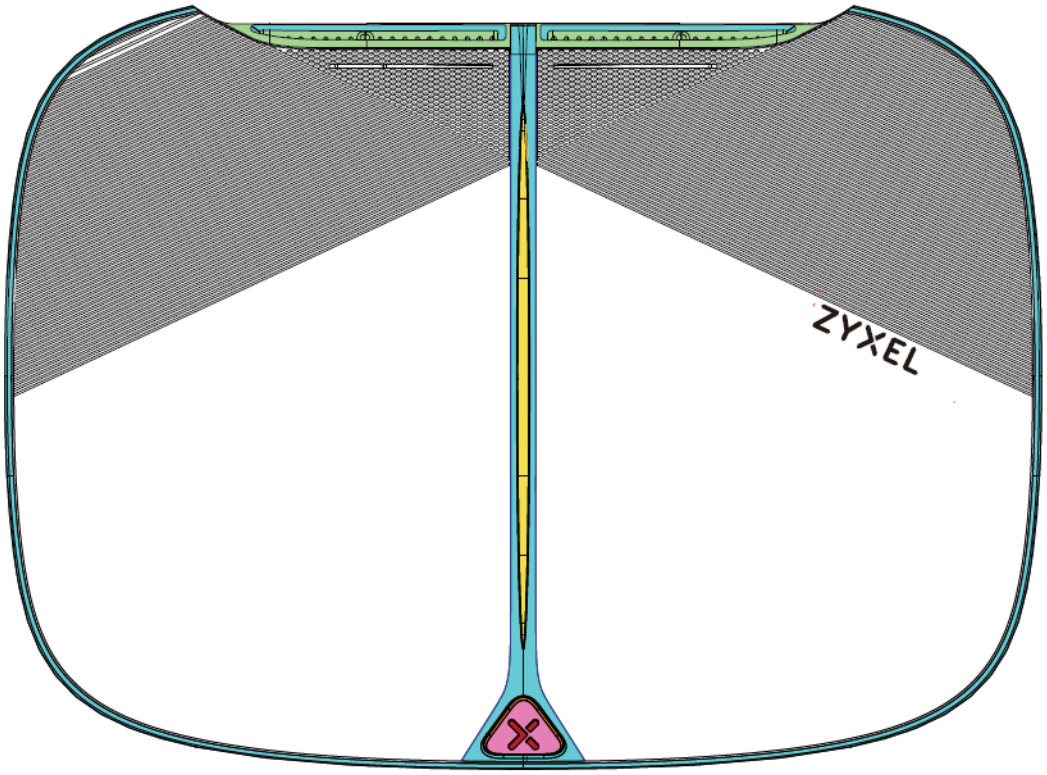
Table 3 Rear Panel Ports

LABEL	DESCRIPTION
Power	Connect the power adapter to start the NBG6818.
USB	The USB port is used for file-sharing and media server.
2.5G/1G	Connect an Ethernet cable to the Ethernet WAN port for Internet access.
LAN1 – LAN4	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
Reset	Press the button for longer than 8 seconds to return the NBG6818 to the factory defaults.

2.2 Front Panel LED

After you connect the power to the NBG6818, view the LEDs to ensure proper functioning of the NBG6818 and as an aid to troubleshooting.

Figure 13 Front Panel LED



The following table describes the front panel LED.

Table 4 Front Panel LED

COLOR	STATUS	DESCRIPTION
White	On	The NBG6818 is receiving power.
	Blinking	The NBG6818 is booting.
Dark Blue	On	Bluetooth is ready.
	Blinking	Bluetooth linking is in process.
Amber	Blinking (Slow)	The NBG6818 is upgrading firmware.
	Blinking (Fast)	The NBG6818 is resetting.
Purple	Blinking	WPS is in process.
Purple and Dark Blue	Blinking	The NBG6818 is receiving power and ready for use.
Red	On	The NBG6818 detects an error while self-testing, or there is a device malfunction.

2.3 Mounting

The NBG6818 can be mounted on the wall or placed on the desk.

2.3.1 Wall Mounting

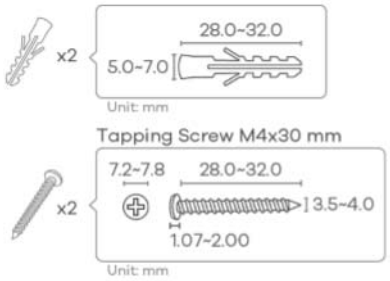
You may need screw anchors if mounting the NBG6818 on a concrete or brick wall.

Table 5 Wall Mounting Information

Distance between holes	10.50 cm
M4 Screws	Two
Screw anchors (optional)	Two

Note: See The WiFi connection is slow or intermittent. when selecting the mounting location.

Figure 14 Screw Specifications



1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.

2 Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

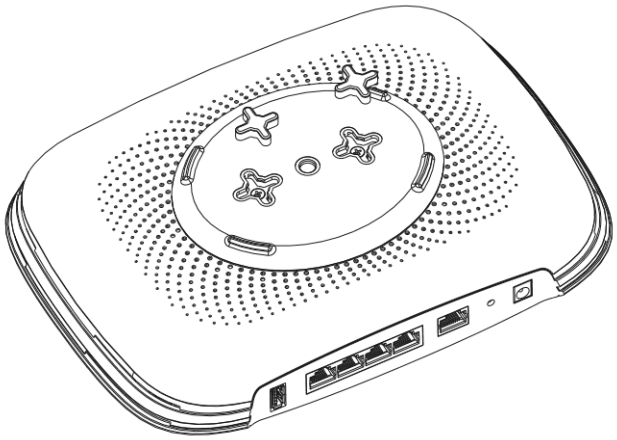
If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

4 Make sure the screws are fastened well enough to hold the weight of the NBG6818 with the connection cables.

5 Remove the rubber feet.

6 Align the holes on the back of the NBG6818 with the screws on the wall. Hang the NBG6818 on the screws.

Figure 15 Wall Mounting- Rubber Feet



2.3.2 Desk Placement

Place the side of the NBG6818 with the attached rubber feet carefully on the desk. These rubber feet help protect the NBG6818 from shock or vibration and ensure space between the desk and NBG6818.

Cautions:

- Ensure enough clearance around the NBG6818 to allow air circulation for cooling.
- Do NOT remove the rubber feet except when wall mounting as it provides space for air circulation.

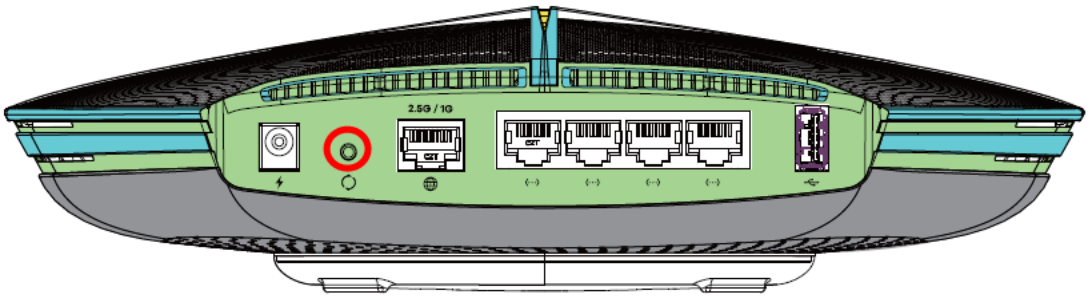
2.4 Resetting the NBG6818

If you forget your password or IP address, or you cannot access the Web Configurator, insert a thin object into the **Reset** hole on the side of the NBG6818 to reload the factory-default configuration file. This means that you will lose all settings that you had previously saved.

2.4.1 How to Use the RESET Button

1. Make sure the power LED is on.
2. Locate the **Reset** hole.
3. Insert a thin object into the **Reset** hole for longer than eight seconds to reset the NBG6818 back to its factory-default configuration (for example, default Standard (Router) operation mode and login IP address of 192.168.123.1, WiFi SSID and password).

Figure 16 Rear Hole



2.5 The WPS Button

Your NBG6818 supports Wi-Fi Protected Setup (WPS), which is an easy way to set up a secure WiFi network. WPS is an industry standard specification, defined by the Wi-Fi Alliance.

WPS allows you to quickly set up a WiFi network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

You can use the WPS button in the Web Configurator of the NBG6818 to activate WPS in order to quickly set up a WiFi network with strong security.

1 Make sure the power LED is on (not blinking).

2 Open the Web Configurator.

3 Click **Settings** > **WiFi** > **WPS**, and the press the WPS button.

4 Press the WPS button on another WPS-enabled device within range of the NBG6818. See the User's Guide of the other device for details.

Note: You must activate WPS on the NBG6818 and on another WiFi device within two minutes of each other.

CHAPTER 3
Wizard

3.1 Wizard Overview

The wizard appears automatically when the NBG6818 is accessed for the first time or when you reset the NBG6818 to its default factory settings. The wizard helps you set up the following:

- 2.4G/5G WiFi name and WiFi password
- Automatically check and update your NBG6818 firmware
- Create a myZyxelCloud account to log into the NBG6818
- Authorize the NBG6818 to access your myZyxelCloud account
- Create a local password as an alternative for logging into the NBG6818.

In this chapter, you will learn how to:

- Go through NBG6818 (ARMOR G1) wizard steps
- Configure basic settings for your WiFi
- Create a myZyxel Cloud account.

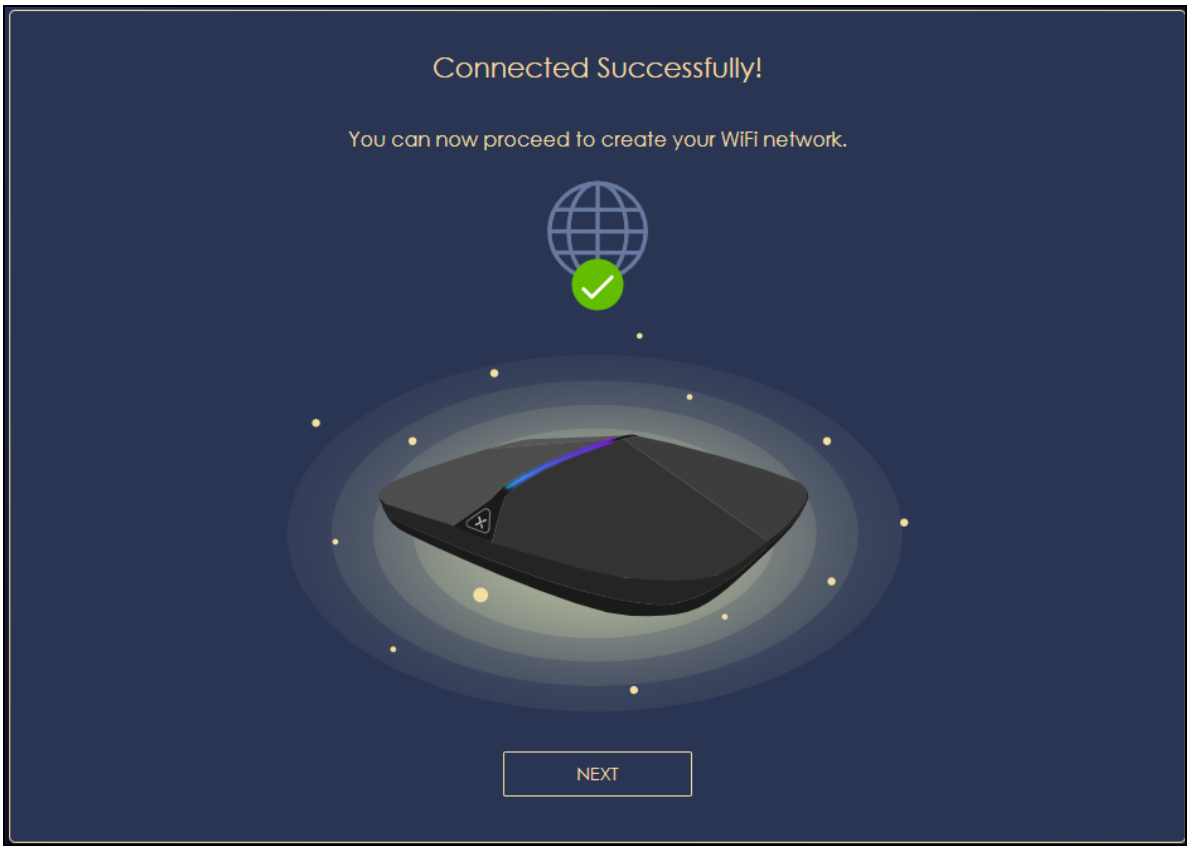
3.2 Accessing the Wizard

Launch your web browser and enter "http://zyxelwifi.com" or "http://zyxelwifi.net" as the website address.

Note: The wizard appears automatically when the NBG6818 is accessed for the first time or when you reset the NBG6818 to its default factory settings.

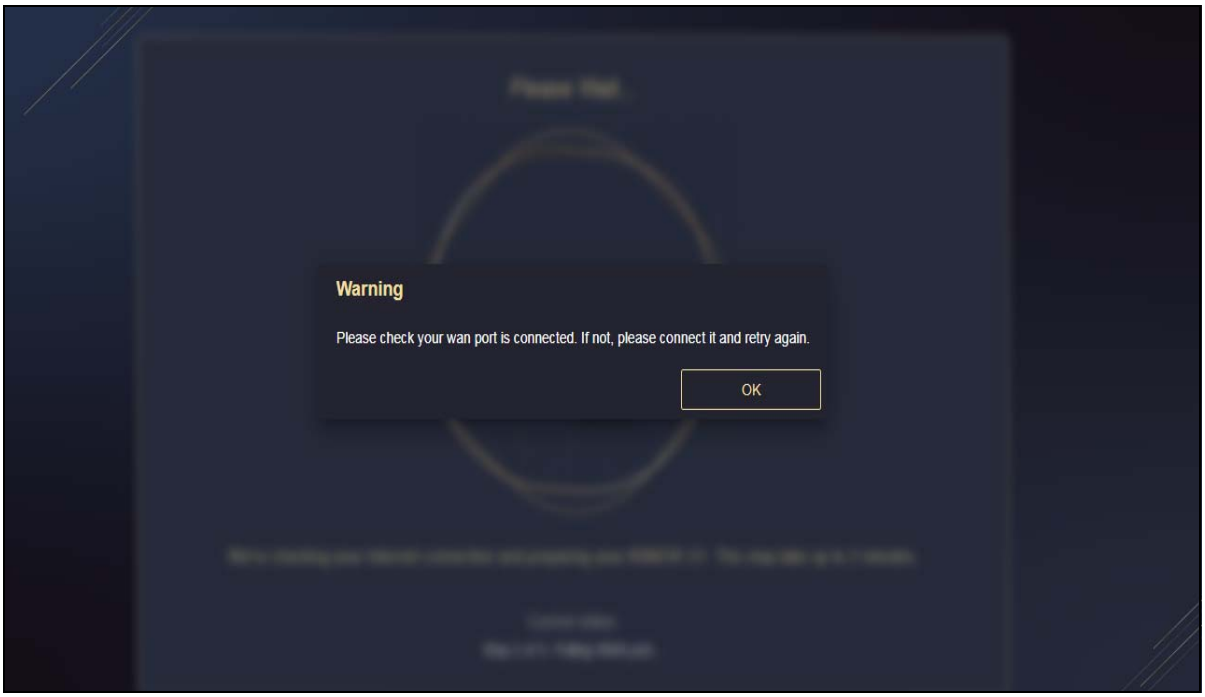
1 Your NBG6818 will check the status of your Internet connection the first time you log in.

2 The following screen shows if you are connected to the Internet. Click **Next** to go to the next step in the wizard.

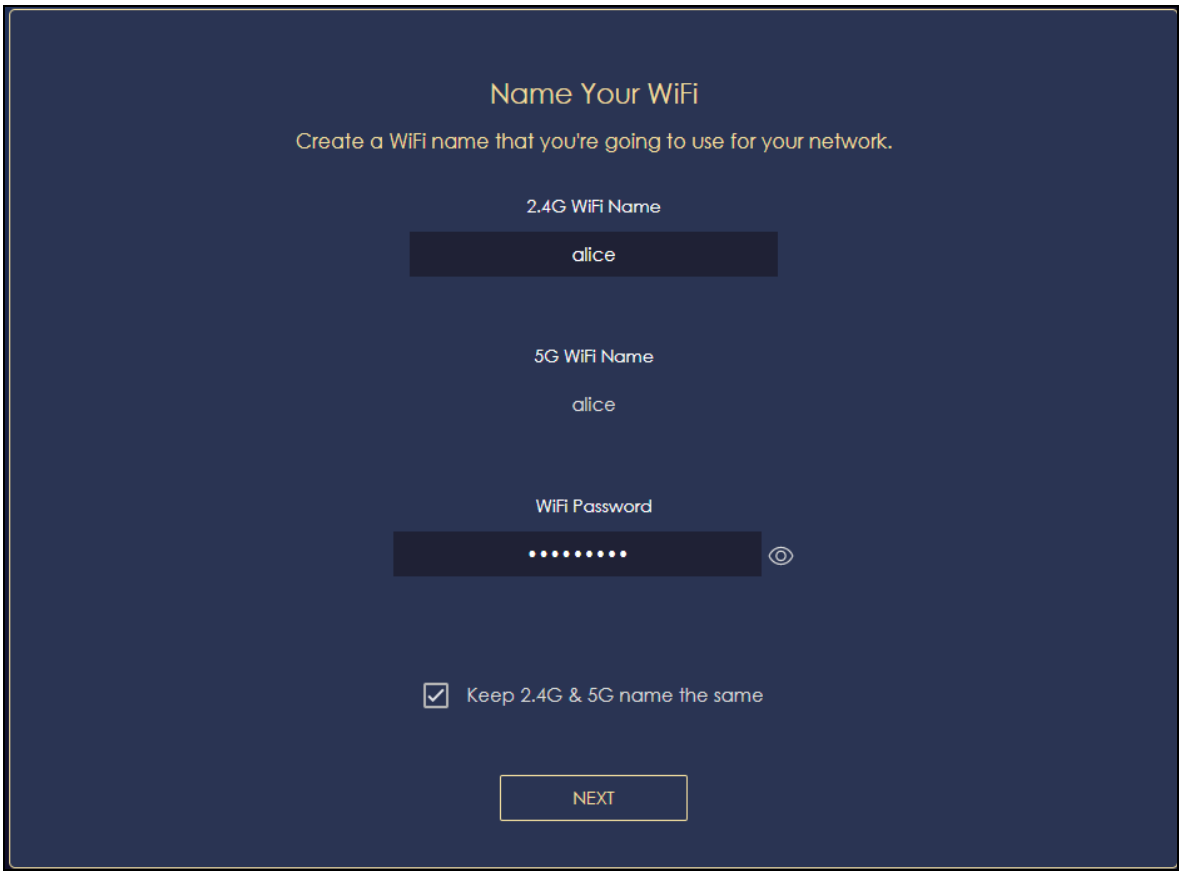


The following screen shows if you are not connected to the Internet.

Note: You may need to turn off your network firewall if access to the Internet from the NBG6818 is blocked. You need to connect to the Internet to access your NBG6818.



3 Enter 1-128 single-byte printable characters but not ""<>^$& as your **2.4G/5G WiFi Name** and **WiFi Password**. Select the check box **Keep 2.4G & 5G name the same** if you want to use the same name for your 2.4G and 5G WiFi.



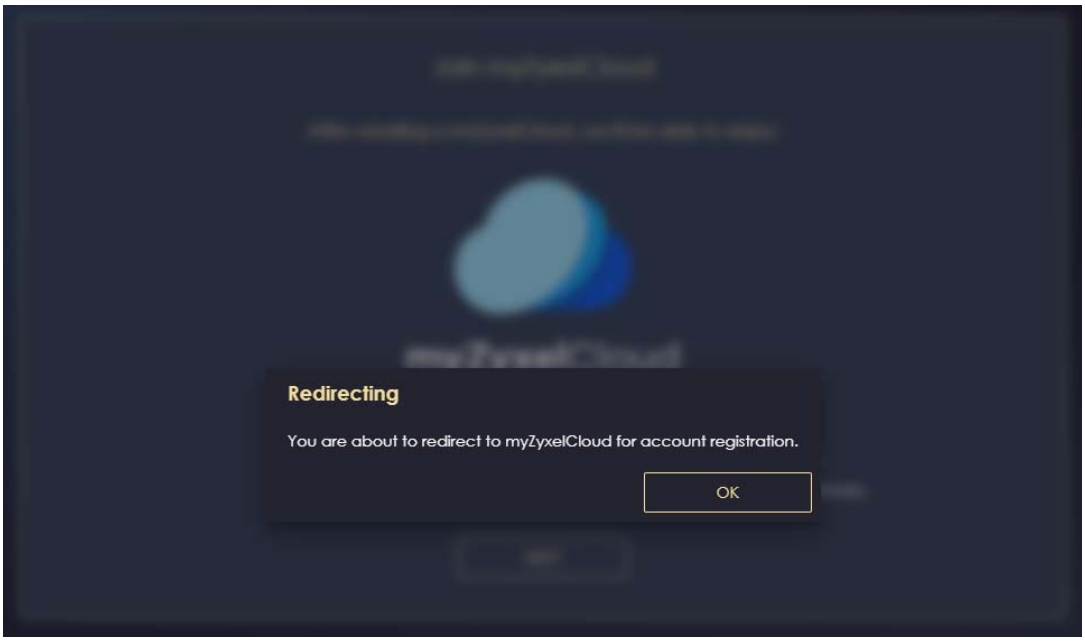
4 Wait a moment for your WiFi settings to be applied to your NBG6818.

5 The following screen shows if you have set up your WiFi name and password successfully. Click **Next** to go to the next step in the wizard.

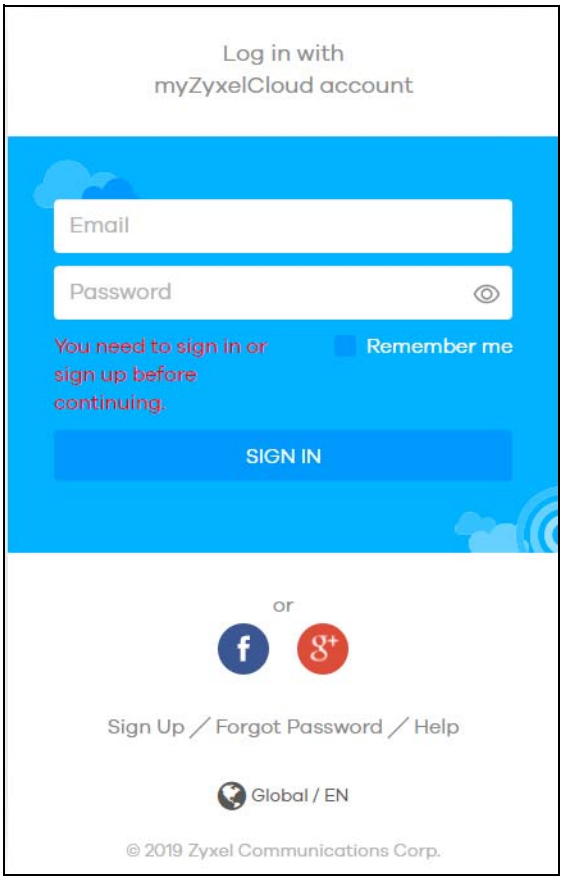
6 Wait a moment for the NBG6818 to check if your device is updated with the latest firmware. If not, your NBG6818 will automatically update the firmware.

7 You need to create a myZyxel Cloud account to log into the NBG6818. The Zyxel cloud service gives you an online management site to configure and view the status of your NBG6818. Click **Next** to go to the next step in the wizard.

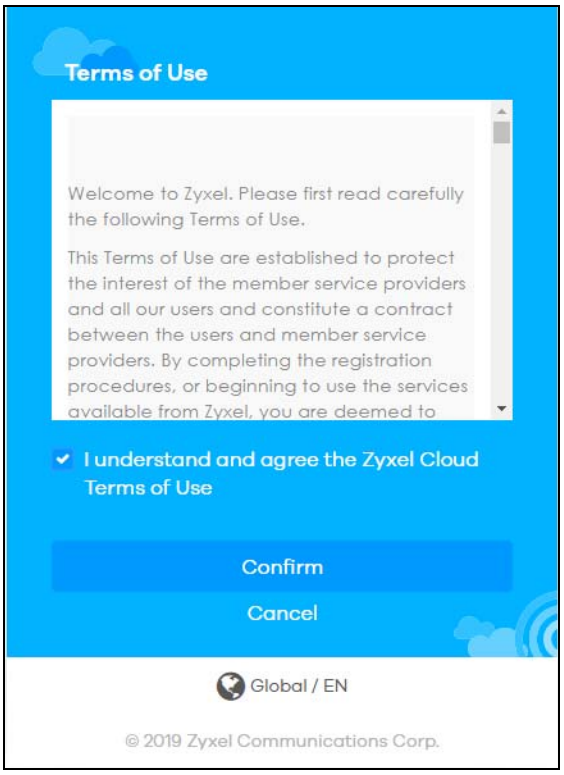
8 A pop-up message shows. Click **OK** to be redirected to the registration website of myZyxel Cloud.



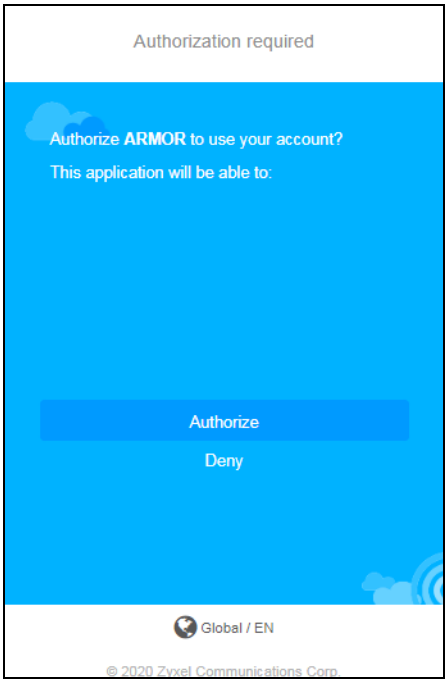
9 Enter your **Email** and **Password** if you already have a myZyxel Cloud account. If not, you can create one by clicking **Sign Up**. You can also click the Facbook or Google icon to create an account with your Facebook or Google account.



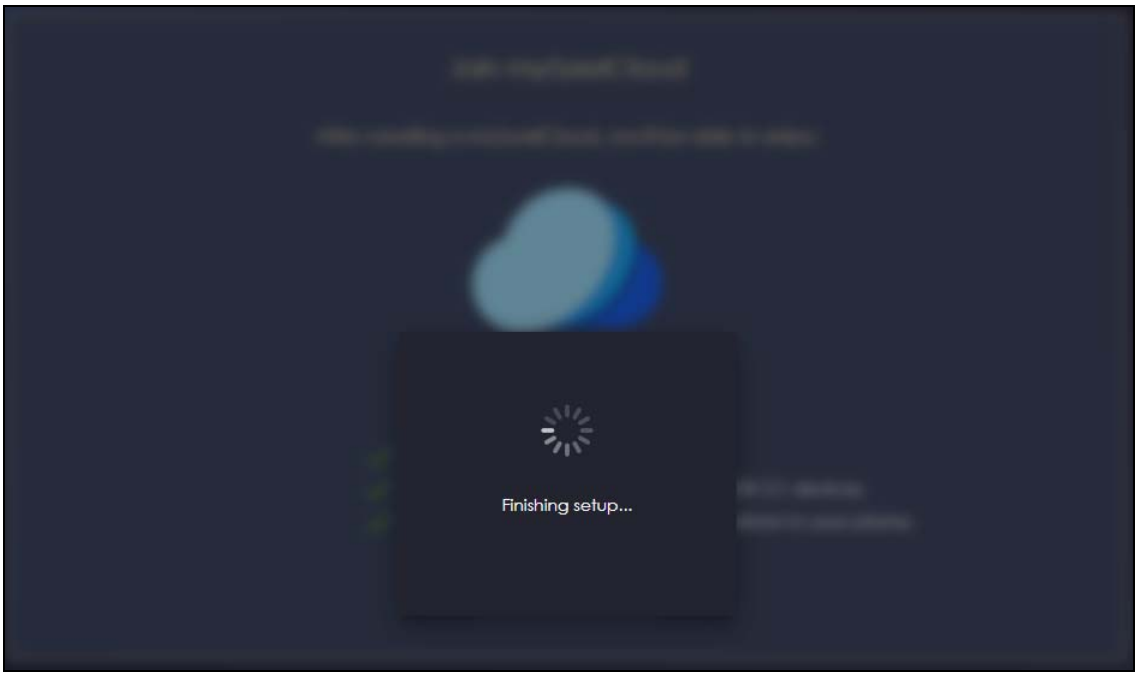
10 The legal page shows after you log in. Select the check box **I understand and agree the Zyxel Cloud Terms of Use** and then click **Confirm**.



11 The following page asks for your authorization to use your account. Click **Authorize** to finish registering your myZyxel Cloud account. You will be directed back to the NBG6818 web configurator.

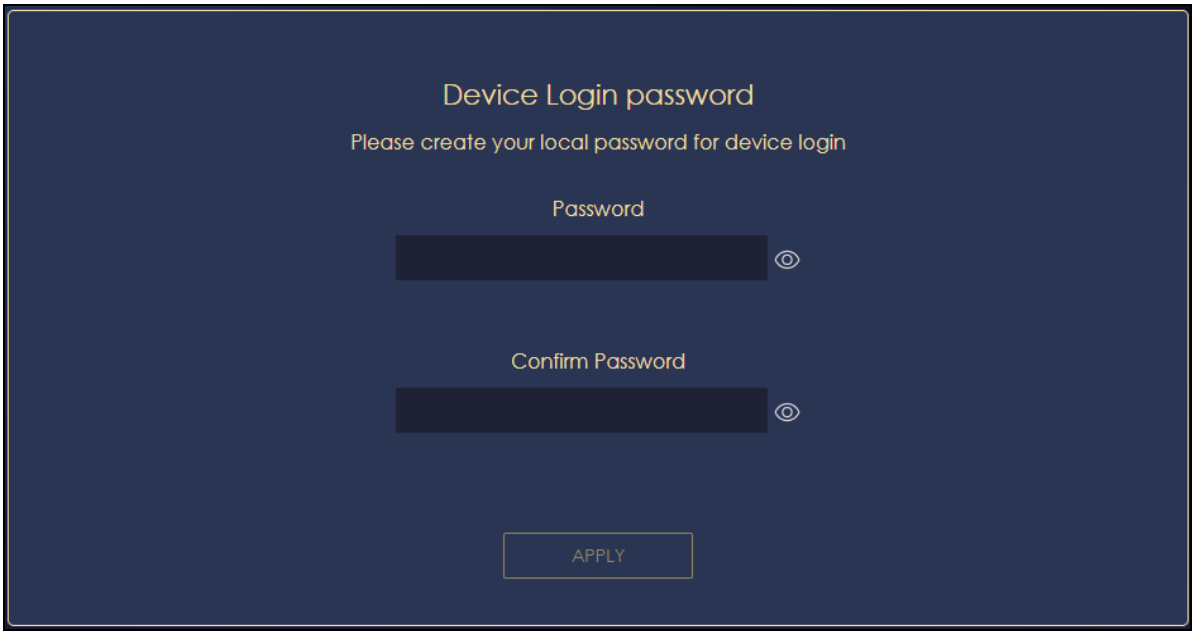


12 Wait a moment for your NBG6818 to link to your myZyxel Cloud account.



13 You can create a local password to access the NBG6818 directly. You can choose to log in with your myZyxel Cloud account or your local password the next time you log in.

Note: You can change your local password in **System** > **General Settings**.



CHAPTER 4
Tutorials

4.1 Tutorials Overview

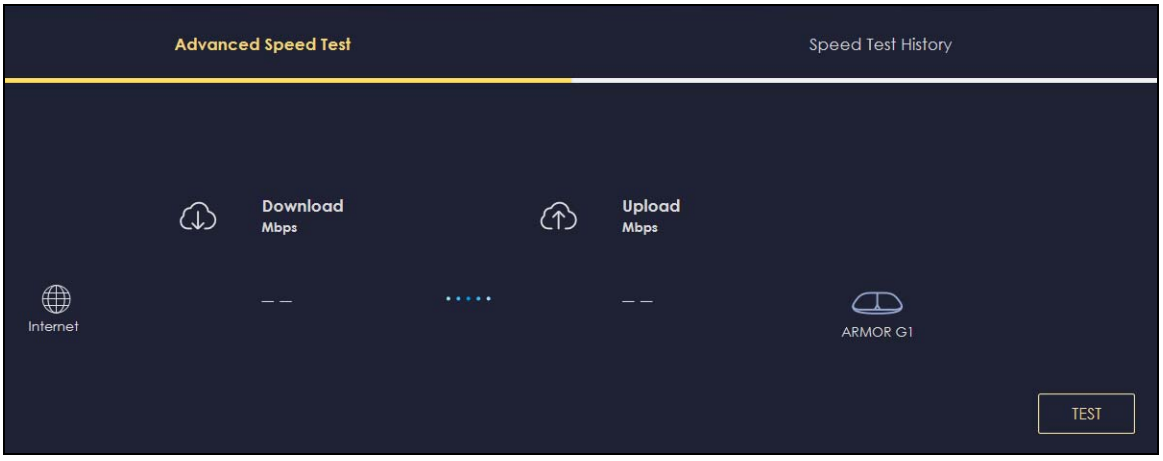
This chapter provides tutorials for setting up your NBG6818.

- Run a Speed Test
- Configure the Main WiFi Network
- Configure the Guest WiFi Network
- Create or Edit a WiFi Schedule Profile
- Add a Client Device to the Profile
- Pause or Resume the Internet Access Using a Profile
- Turn on or off the NBG6818's LED (Light)
- Change Your NBG6818 Operating Mode
- Configure a Port Forwarding Rule
- Configure NBG6818 as an OpenVPN Server
- Configure NBG6818 as an OpenVPN Client

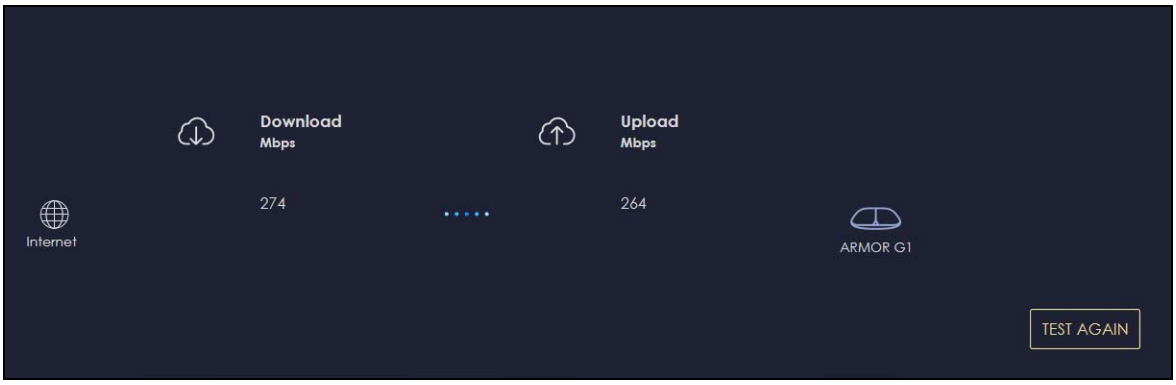
4.2 Run a Speed Test

Use the **Advanced Speed Test** screen to check the speed of the connection between your NBG6818 and the broadband modem/router.

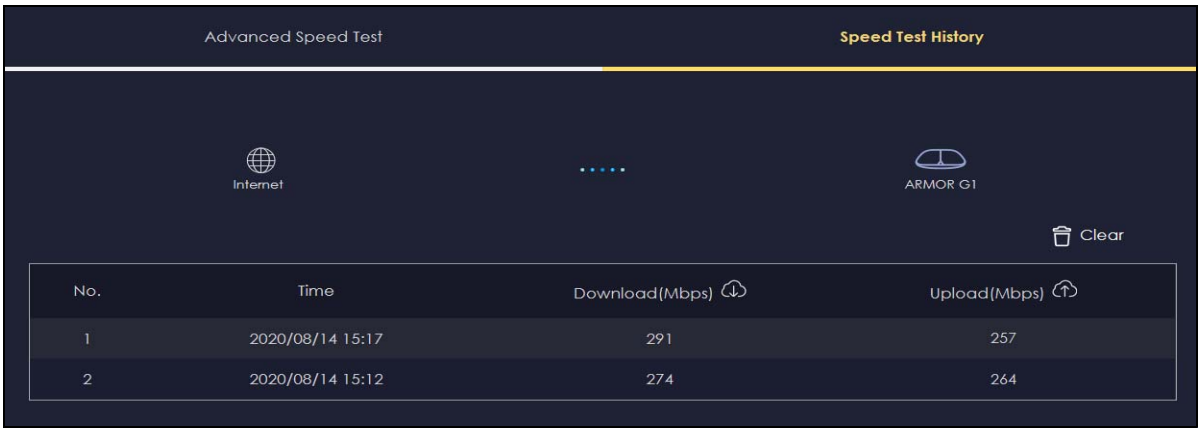
1 Click the **Navigation Panel** icon on the top-left corner ( ), and then select **Diagnose**. The **Advanced Speed Test** screen appears. Click **TEST** to perform a speed test.



2 The test result shows data rates of both upstream and downstream traffic. Click **TEST AGAIN** to update the information in this screen.



3 Click the **Speed Test History** tab to view the summary of the previous tests. Click **Clear** to delete all results.



4.3 Configure the Main WiFi Network

You can set up Main and Guest WiFi network settings on the NBG6818. The following table shows the functions and privileges of the Main and Guest WiFi networks.

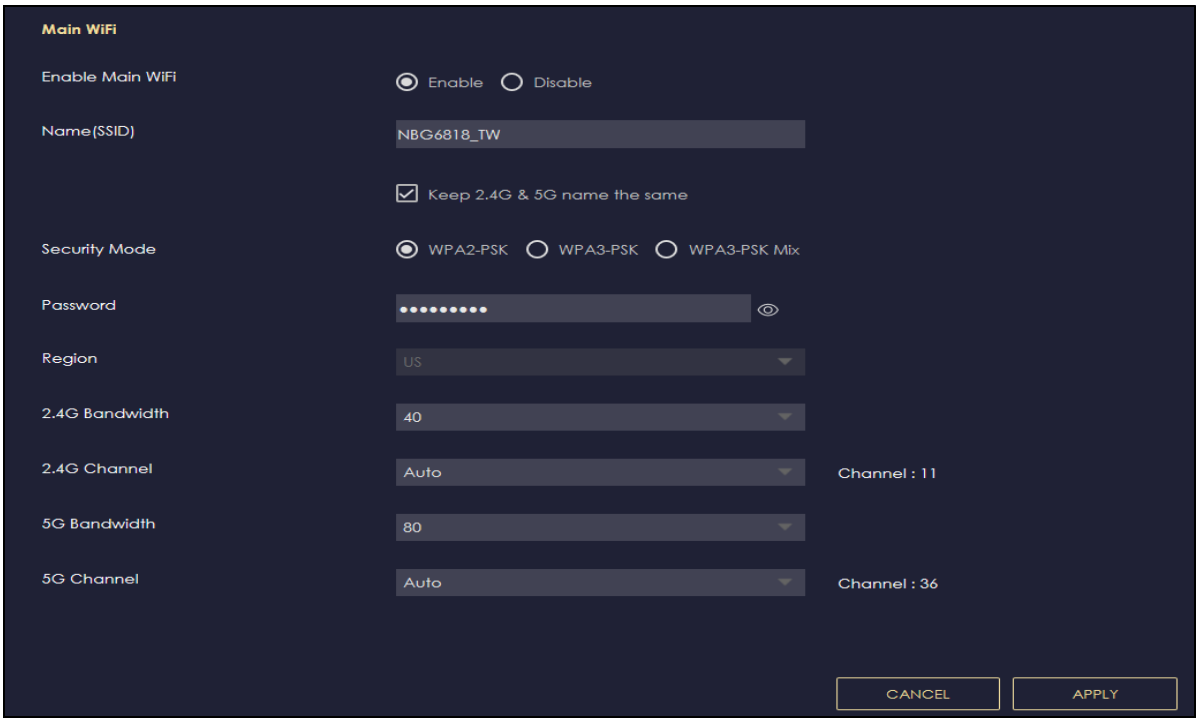
Table 6 WiFi Network Privileges

WIFI NETWORK	INTERNET ACCESS	2.4G / 5G WIFI NETWORK	ACCESS TO WEB CONFIGURATOR	ACCESS TO WIRED LAN
Main WiFi	Yes	2.4G and 5G	Yes	Yes
Guest WiFi	Yes	2.4G and 5G	No	No

Note: A user can only configure the WiFi networks' security settings if they are connected to the **Main WiFi** network.

1 Click the **Navigation Panel** icon on the top-left corner ( ), and then select **Settings** to open the **WiFi** screen. Use the tabs in the **WiFi** menu to configure WiFi networks' security settings.

2 Select **Enable** to activate the **Main WiFi** network on the **Main WiFi** screen. Enter the 2.4G/5G **Name (SSID)** and **Password** . You can use two different **Name (SSID)** for the 2.4G and 5G **Main WiFi** networks. If you want the 2.4 G and 5G WiFi to use the same SSID, select **Keep 2.4G & 5G name the same**. Use this screen to configure the WiFi security mode, bandwidth, and channel for the 2.4 G and 5 G networks. Click **APPLY** to save your changes.



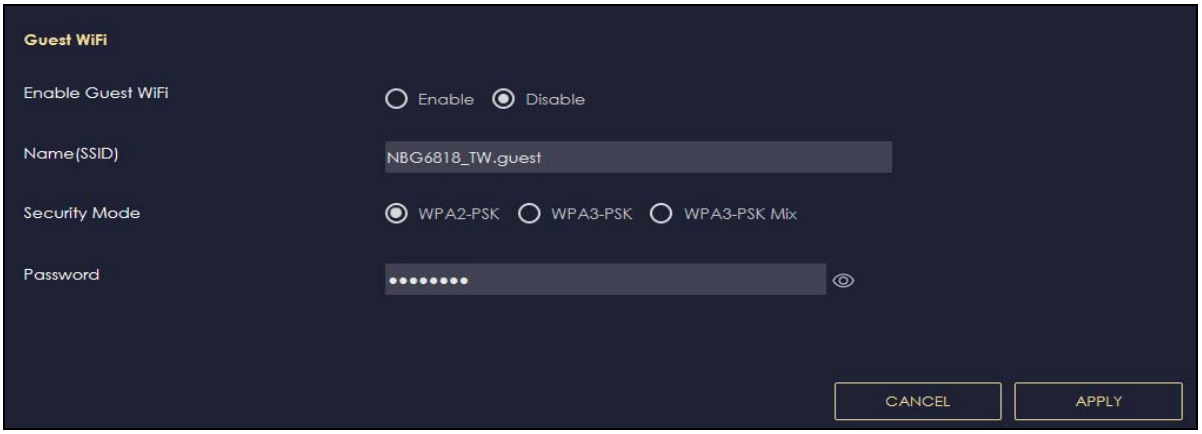
4.4 Configure the Guest WiFi Network

Use this screen to configure **Guest WiFi** networks for your clients.

Note: This is not available if you are using bridge mode.

1 Click the **Navigation Panel** icon on the top-left corner ( ), and then select **Settings** to open the **WiFi** screen.

2 Click the **Guest WiFi** tab on the **Settings > WiFi > Guest WiFi** screen. The following screen appears. Select **Enable** to activate **Guest WiFi**. Enter the Guest WiFi **Name (SSID)** and WiFi **Password**. Select **WPA2-PSK**, **WPA3-PSK** or **WPA3-PSK Mix** mode to add a layer of security to this WiFi network. Click **APPLY** to save your changes.



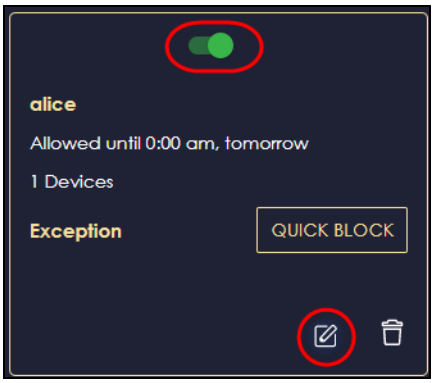
4.5 Create or Edit a WiFi Schedule Profile

Create a profile to quickly block or allow the WiFi access of a client device using a profile.

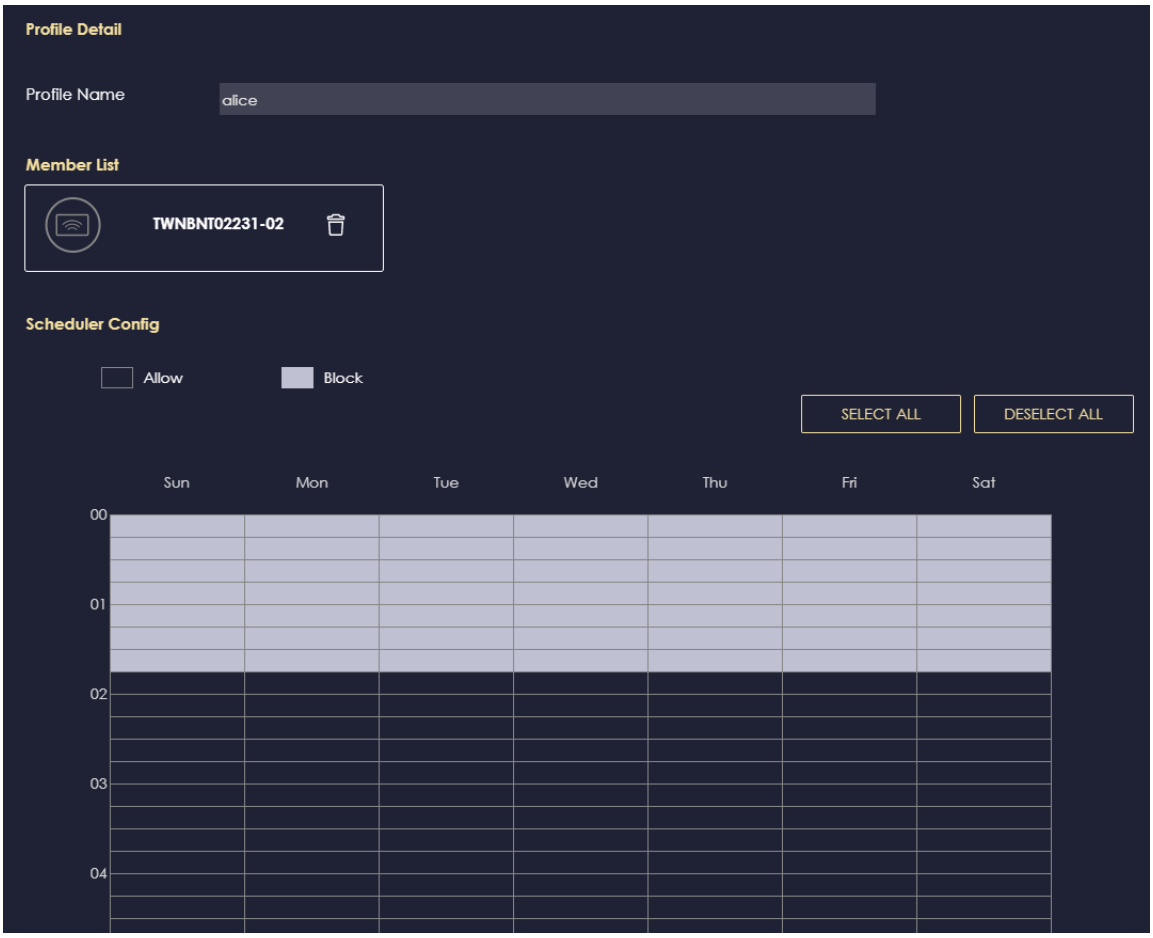
Note: This is not available if you are using bridge mode.

1 Click the **Navigation Panel** icon on the top-left corner ( ). Select **Parental Control**, and click the **Profile** tab. Use the **Profile** screen to view the predefined profiles.

2 Click the switch to enable the profile. Click the **QUICK BLOCK** button to block the client device from using this profile. Click the **Edit** icon ( ) if you want to modify the profile's Internet schedule.



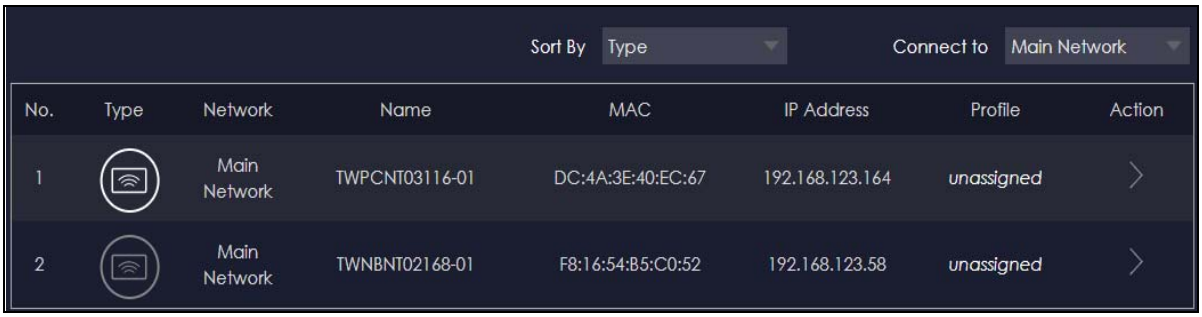
3 The following screen appears after you click the **Edit** icon ( ). Select the **Block** check box on the **Profile Detail** screen. Select a time slot and drag it down to create a blocking schedule for your client. Alternatively, select the **Allow** check box and create a schedule to allow the WiFi access for your client device.



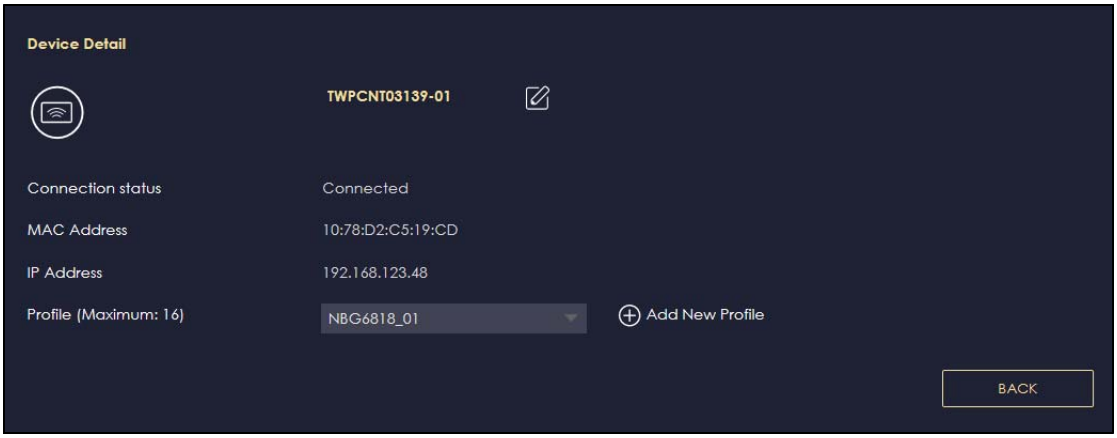
4.6 Add a Client Device to the Profile

Use this screen to quickly block or resume Internet access and configure a schedule for WiFi clients.

1 Click the **Navigation Panel** icon on the top-left corner ( ), and then select **Parental Control**. The following screen appears. Use this screen to view client devices connected to your NBG6818.



2 Click the Action ( ) icon of a client device to view the details of the client device information. The following screen appears. On the **Device Detail** screen**,** select a predefined profile from the drop-down list box to apply a profile to the client device. Cick **BACK** to return to the previous screen. Click **Add New Profile** if you want to create a new profile.



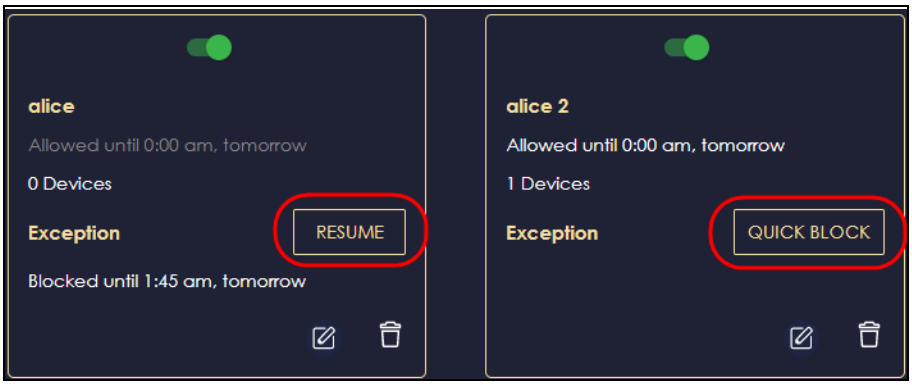
4.7 Pause or Resume the Internet Access Using a Profile

Use this screen to block client devices from accessing WiFi or resume WiFi access immediately.

Note: This is not available if you are using bridge mode.

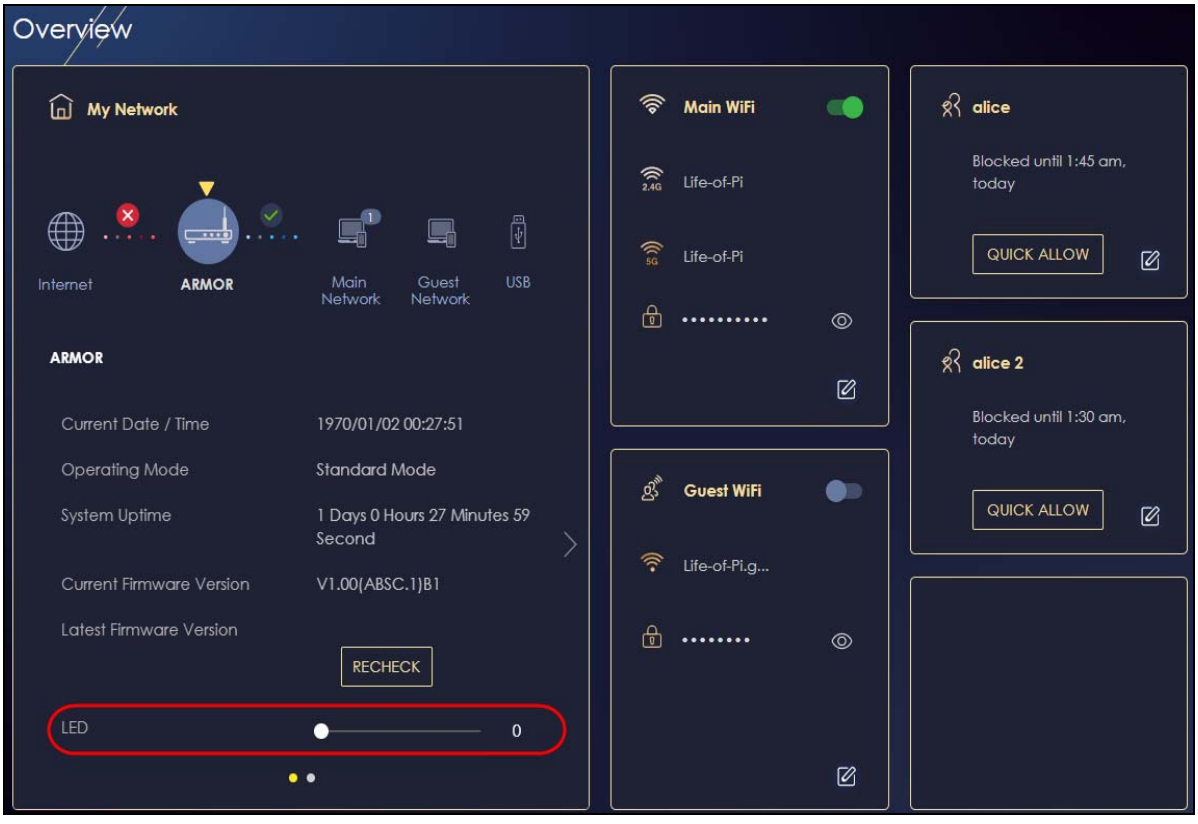
1 Click the **Navigation Panel** icon on the top-left corner ( ). Select **Parental Control**, and click the **Profile** tab. Use the **Profile** screen to view the profiles created.

2 Click the **RESUME** button to allow network access at once. Click the **QUICK BLOCK** button to block Internet access immediately using this profile.



4.8 Turn on or off the NBG6818's LED (Light)

In the **Overview** screen, find the **LED** field and drag the button of the slider to increase the brightness or turn off the NBG6818's LED.



4.9 Change Your NBG6818 Operating Mode

You can use the NBG6818 as a router or bridge. The NBG6818 has the following operating modes:

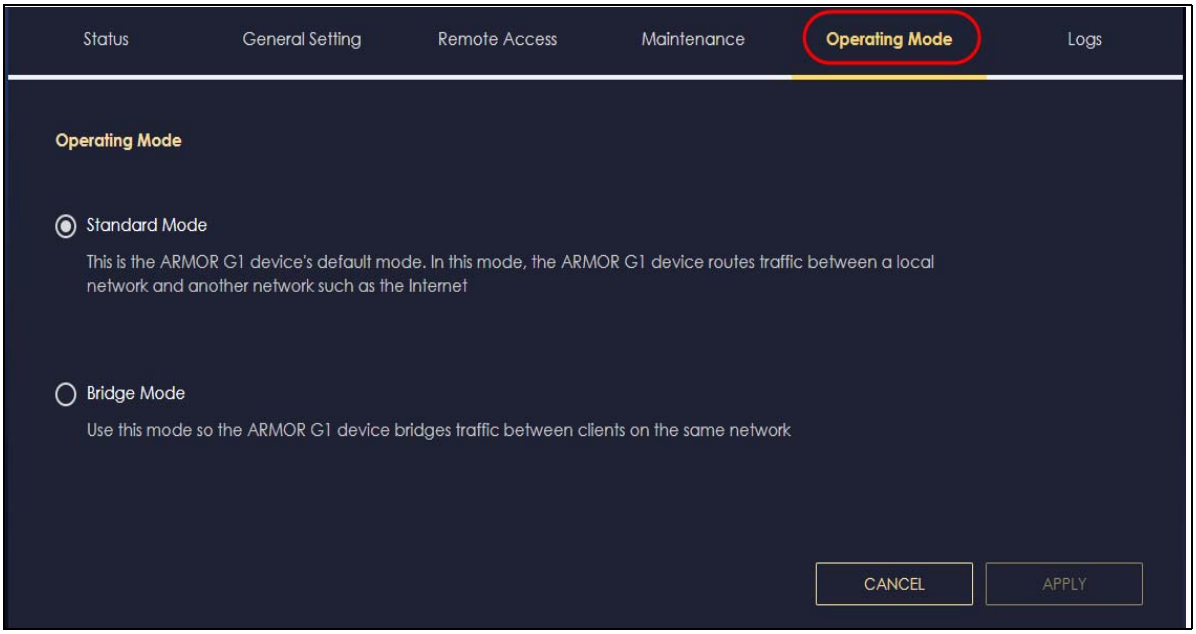
- **Standard:** This is the NBG6818's default mode. In this mode, the NBG6818 routes traffic between a local network and another network such as the Internet.
- **Bridge:** Use this mode so the NBG6818 bridges traffic between clients on the same network.

Note: Features such as parental Control, UPnP, Port Forwarding are not available in Bridge mode.

1 Click the **Navigation Panel** icon on the top-left corner ( ).

2 From the **Settings** drop-down list, click **System**, then click the **Operating Mode** tab.

3 Select the operating mode and select **APPLY** to save your changes. Changing the NBG6818's operating mode may take up to two minutes.

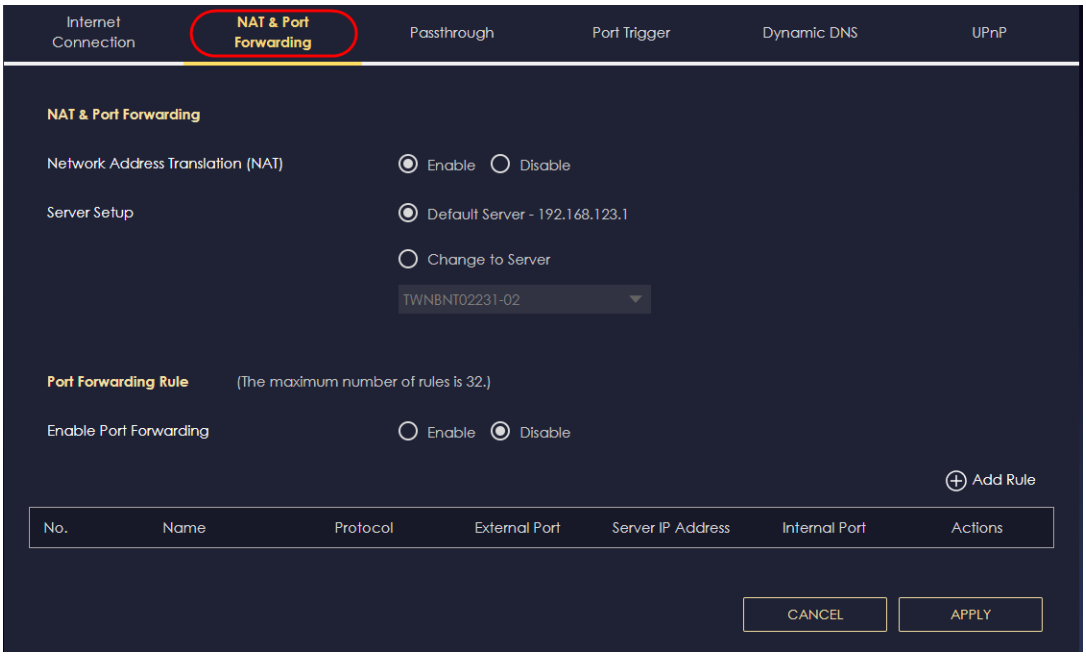


4.10 Configure a Port Forwarding Rule

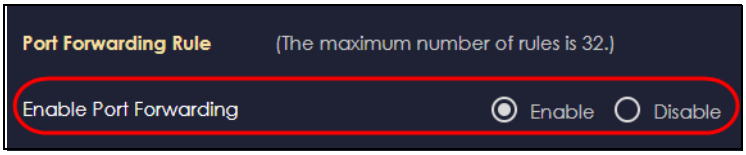
If you want to forward incoming packets to a computer on the LAN using ports, create a port forwarding rule.

Note: This is not available if you are using bridge mode.

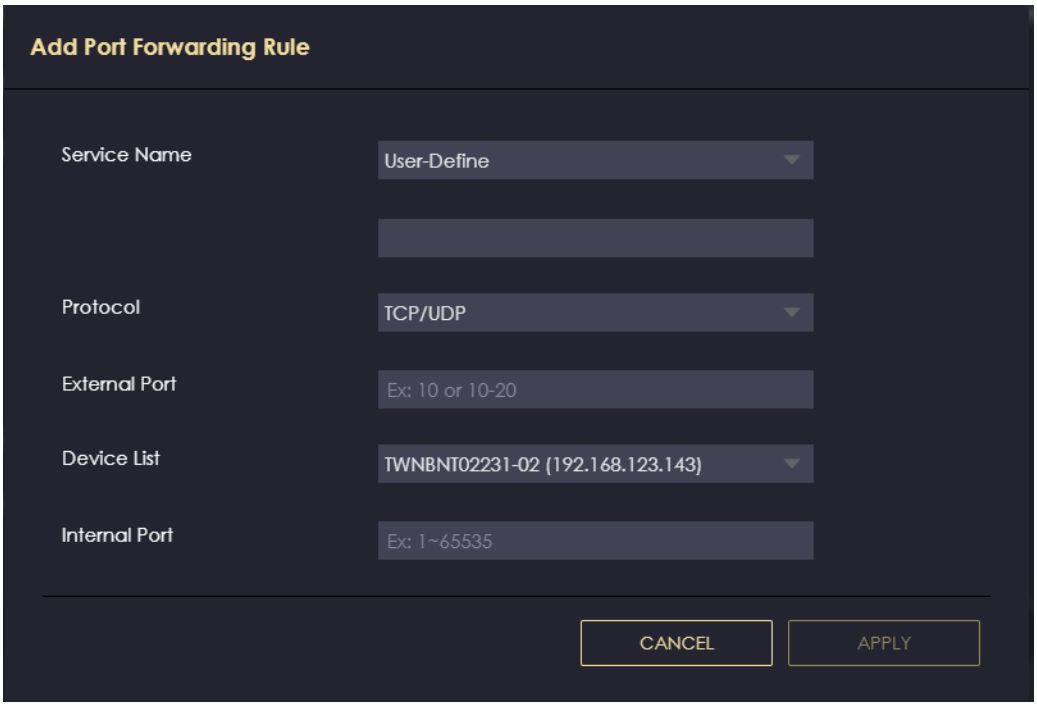
1 Click the **Navigation Panel** icon on the top-left corner ( ). From the **Settings** drop-down list, select **Internet**, and click the **NAT & Port Forwarding** tab.



2 Select **Enable** in the **Enable Port Forwarding** field.



3 Click **Add Rule** to create a port forwarding rule. Add a service name, a port number or a range of ports to define the service to be forwarded, specify the transport layer protocol used for the service, and the IP address of a computer on your LAN that will receive the packets from the ports.

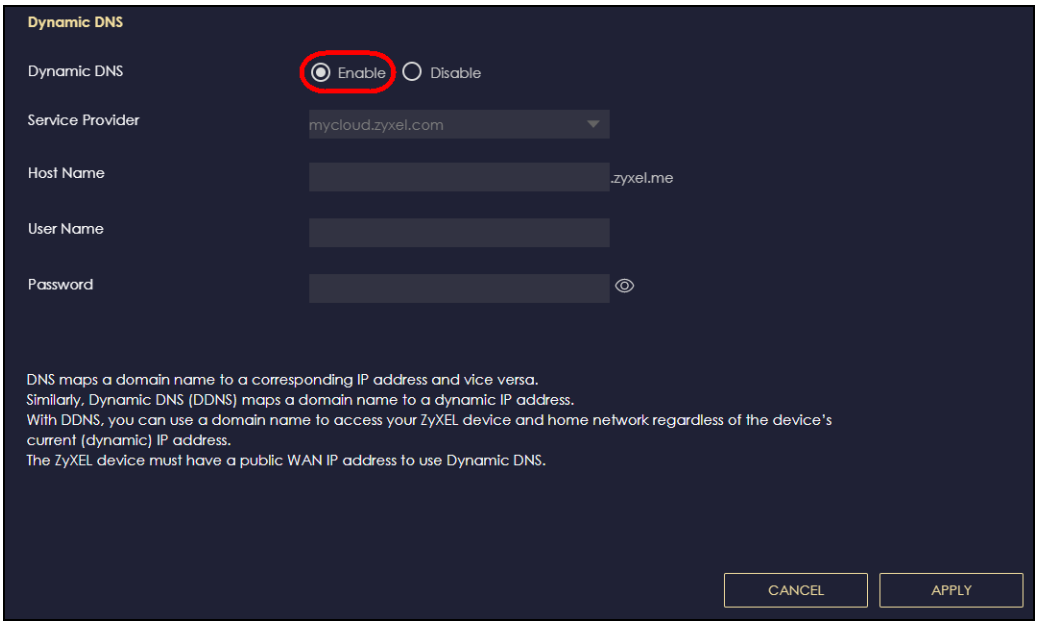


4.11 Configure NBG6818 as an OpenVPN Server

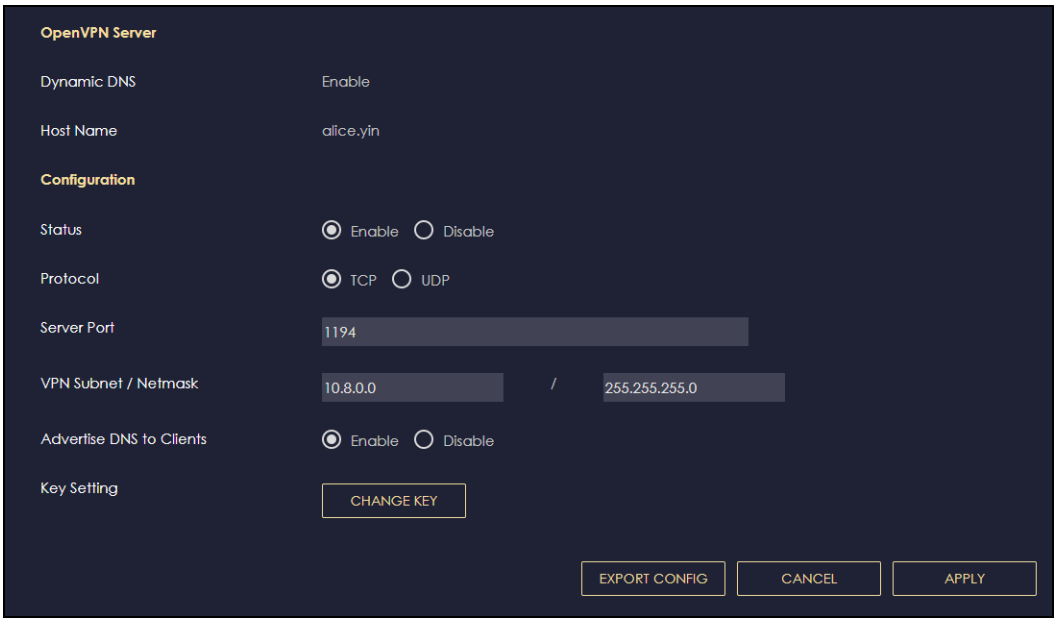
Create an OpenVPN server account to allow the NBG6818 to transmit data to client devices through a secure VPN channel.

Note: This is NOT available if you are using bridge mode.

1 Enable DDNS (Dynamic DNS) in **Settings** > **Internet** > **Dynamic DNS**. Click **APPLY**.

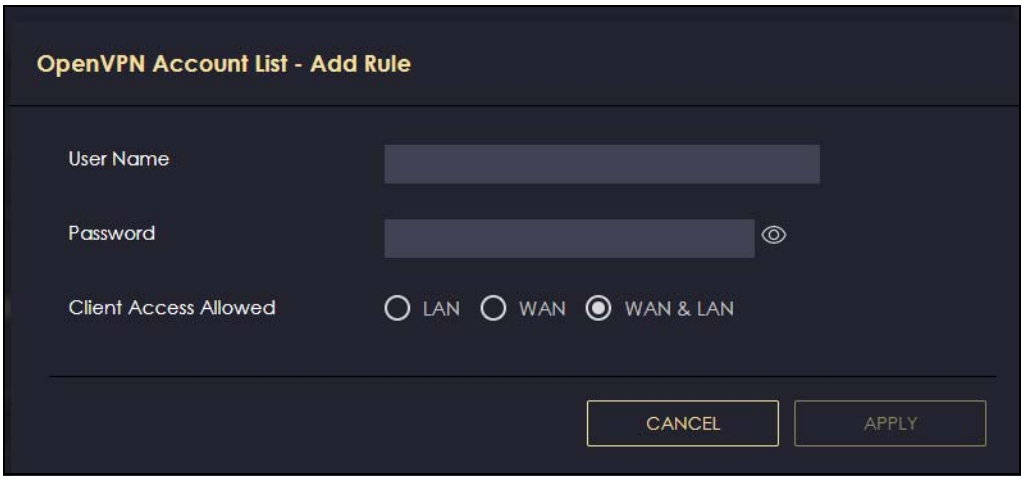


2 Click the **Navigation Panel** icon on the top-left corner ( ). Select **OpenVPN Server**, and click the **OpenVPN Server** tab. Configure the OpenVPN Server account.



3 Click the **OpenVPN Account** tab.

4 Click **Add Rule** to create up to 5 OpenVPN account rules. Add a user name, set the password, and select the interfaces through which the clients are allowed to connect to the account.

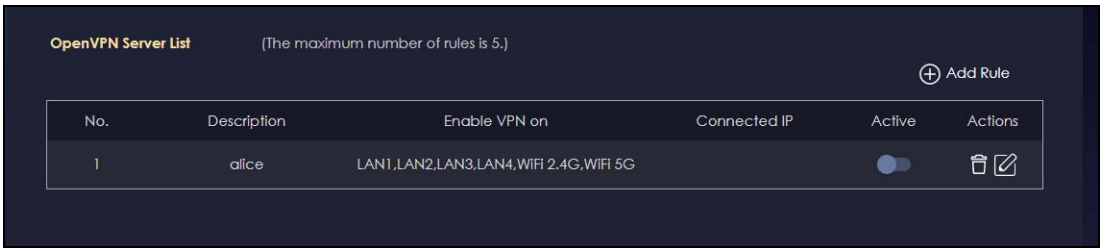


4.12 Configure NBG6818 as an OpenVPN Client

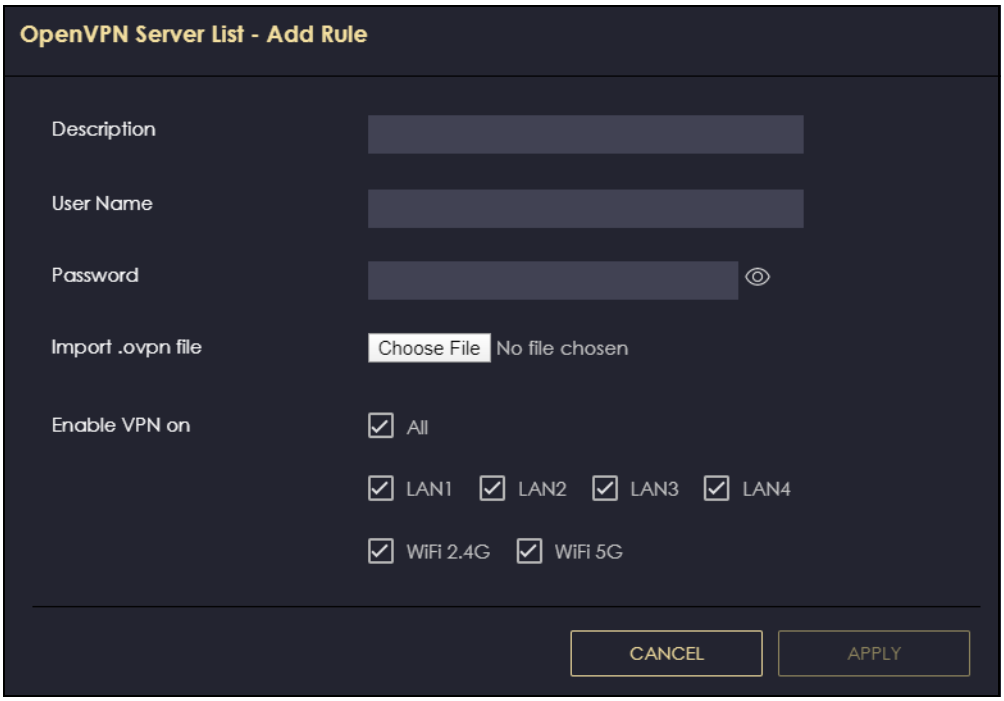
Use OpenVPN Client to allow a VPN server to transmit data through a secure VPN channel to the NBG6818 client device.

Note: Do NOT activate OpenVPN Server and OpenVPN Client at the same time. The NBG6818 can only connect to one server at a time.

1 Click the **Navigation Panel** icon on the top-left corner ( ). Select **OpenVPN Client**.



2 Click **Add Rule** to create up to 5 OpenVPN account rules. Add a description, user name and password of the OpenVPN Server, import an .ovpn file that you get from the OpenVPN Server that you want to connect to, and select the interfaces that are allowed by the OpenVPN Server account.


OpenVPN Server List - Add Rule
Description
User Name
Password
Import .ovpn file
Choose File
No file chosen
Enable VPN on
All
LAN1
LAN2
LAN3
LAN4
WiFi 2.4G
WiFi 5G
CANCEL
APPLY

CHAPTER 5
The Web Configurator

5.1 Overview

This chapter describes how to access the NBG6818 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy system setup and management via Internet browser. Use a browser that supports HTML5, such Mozilla Firefox, or Google Chrome. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device
- JavaScript (enabled by default)
- Java permissions (enabled by default).

5.2 Accessing the Web Configurator

1. Make sure your NBG6818 hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. If the NBG6818 is in **Standard Mode** (the default mode), enter "http://zyxelwifi.com" in the browser's address bar.

   If the NBG6818 is in **Bridge Mode**, enter "http:// (DHCP-assigned IP)" in the browser's address bar.
4. On the displayed login screen, log in using your myZyxelCloud username and password or the local password.

   Note: If this is the first time you are accessing the web configurator or if the device has been reset, you must complete the setup wizard, see Chapter 3 on page 25.

   Note: For setting and changing the local password, see Section 13.4 on page 137.

Figure 17 LOG IN

5 The NBG6818 **Overview** screen displays allowing you to monitor your NBG6818. It shows if the NBG6818 is online, and how many WiFi clients are currently connected to your device, as well as their upstream/ downstream data rates.

Figure 18 Overview (Standard Mode)

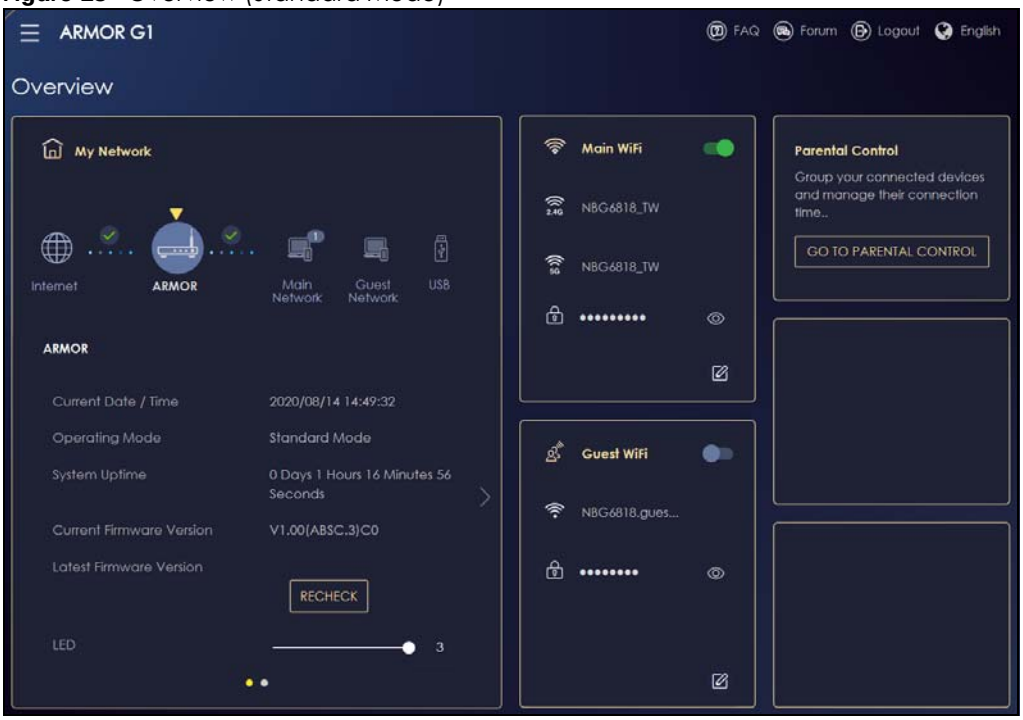
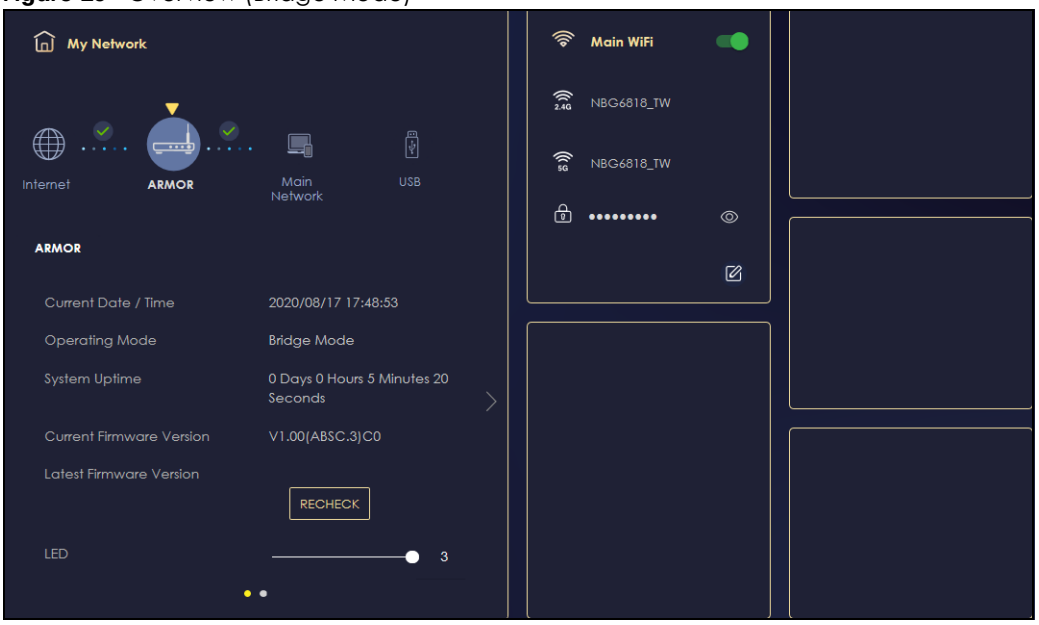


Figure 19 Overview (Bridge Mode)

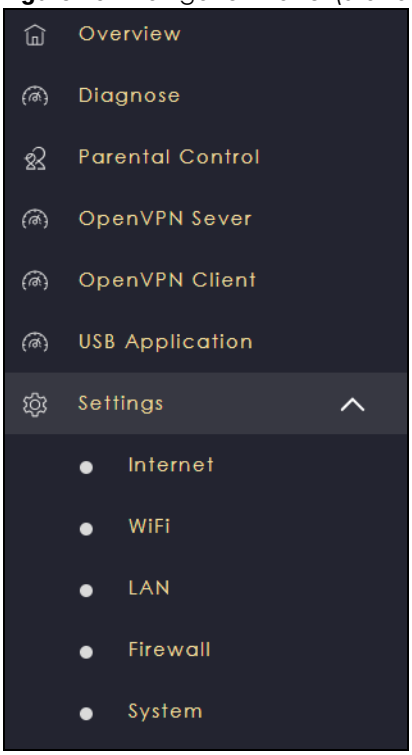


5.3 Navigation Panel

Use the submenus on the navigation panel to configure NBG6818 features. Your navigation panel varies depending on the mode of your NBG6818.

5.3.1 Standard Mode Navigation Panel

Figure 20 Navigation Panel (Standard Mode)



The following table describes the submenus.

Table 7 Settings > System > Status (Standard Mode)

LINK	TAB	FUNCTION
Overview		Use this screen to: • View read-only information about your NBG6818 • Configure WiFi settings • Change the brightness of your device's LED.
Diagnose	Advanced Speed Test	Use this screen to check the speed of the connection between your NBG6818 and the broadband modem/router.
	Speed Test History	Use this screen to view a summary of previous speed tests.
Parental Control	Device	Use this screen to: • View devices information • Add and configure parental control rules or schedules.
	Profile	Use this screen to enable or configure existing parental control rules.
OpenVPN Server	OpenVPN Server	Use this screen to create and configure an OpenVPN server account.
	OpenVPN Account	Use this screen to: • View basic information about NBG6818 OpenVPN server • View basic information about clients that are connected to the NBG6818 OpenVPN server.

Table 7 Settings > System > Status (Standard Mode) (continued)

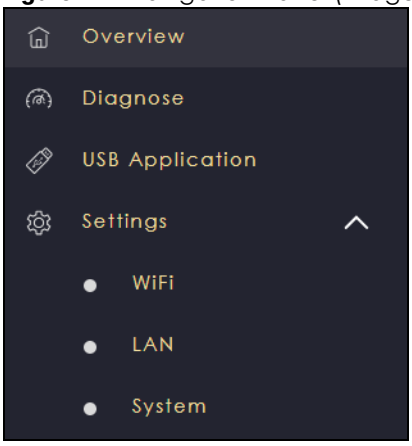
LINK	TAB	FUNCTION
OpenVPN Client		Use this screen to: • View basic information about OpenVPN Server accounts that you are connected to • Add an OpenVPN Server Account you want your NBG6818 to connect to when the NBG6818 functions as an OpenVPN client.
USB Application	SAMBA	Use this screen to: • Set up file-sharing via the NBG6818 using Windows Explorer or the workgroup name • Configure the workgroup name and create file-sharing user accounts.
	FTP	Use this screen to set up file sharing via the NBG6818 using FTP and create user accounts.
	USB Media Sharing	Use this screen to configure settings for media sharing.
Internet	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	NAT & Port Forwarding	Use this screen to enable NAT. Use this screen to configure servers behind the NBG6818 and forward incoming service requests to the servers on your local network.
	Passthrough	Use this screen to change your NBG6818's port triggering settings.
	Port Trigger	Use this screen to configure ALGs (Application Layer Gateway) and VPN pass-through settings.
	Dynamic DNS	Use this screen to configure dynamic DNS.
	UPnP	Use this screen to enable UPnP on the NBG6818.
WiFi	Main WiFi	Use this screen to enable the wireless LAN and configure wireless LAN and WiFi security settings.
	Guest WiFi	Use this screen to configure multiple BSSs on the NBG6818.
	MAC Filter	Use the MAC filter screen to configure the NBG6818 to block access to devices or block the devices from accessing the NBG6818.
	WPS	Use this screen to configure WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	LAN IP	Use this screen to configure the NBG6818's LAN IP address and subnet mask. Use this screen to configure the IPv6 address for the NBG6818 on the LAN. Use this screen to enable the NBG6818's DHCP server.
	IPv6 LAN	Use this screen to configure the IPv6 address for your NBG6818 on the LAN.
Firewall	IPv4 Firewall	Use this screen to configure IPv4 firewall rules.
	IPv6 Firewall	Use this screen to configure IPv6 firewall rules.

Table 7 Settings > System > Status (Standard Mode) (continued)

LINK	TAB	FUNCTION
System	Status	Use this screen to view the basic information of the NBG6818.
	General Setting	Use this screen to change password or to set the timeout period of the management session.
	Remote Access	Use this screen to configure the interface/s from which the NBG6818 can be managed remotely and specify a secure client that can manage the NBG6818.
	Maintenance	Use this screen to upload firmware, reboot the NBG6818 without turning the power off or reset the NBG6818 to factory default.
	Operating Mode	Use this screen to select whether your device acts as a router, or a bridge.
	Logs	Use this screen to view the list of activities recorded by your NBG6818.

5.3.2 Bridge Mode Navigation Panel

Figure 21 Navigation Panel (Bridge Mode)



The following table describes the submenus.

Table 8 Settings > System > Status (Bridge Mode)

LINK	TAB	FUNCTION
Overview		Use this screen to: • View read-only information about your NBG6818 • Configure WiFi settings • Change the brightness of your device's LED.
Diagnose	Advanced Speed Test	Use this screen to check the speed of the connection between your NBG6818 and the broadband modem/router.
	Speed Test History	Use this screen to view a summary of previous speed tests.
USB Application	SAMBA	Use this screen • Set up file-sharing via the NBG6818 using Windows Explorer or the workgroup name • Configure the workgroup name and create file-sharing user accounts.
	FTP	Use this screen to set up file sharing via the NBG6818 using FTP and create user accounts.
	USB Media Sharing	Use this screen to configure settings for media sharing.

Table 8 Settings > System > Status (Bridge Mode) (continued)

LINK	TAB	FUNCTION
WiFi	Main WiFi	Use this screen to enable the wireless LAN and configure wireless LAN and WiFi security settings.
	MAC Filter	Use the MAC filter screen to configure the NBG6818 to block access to devices or block the devices from accessing the NBG6818.
	WPS	Use this screen to configure WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	LAN IP	Use this screen to configure the NBG6818's LAN IP address and subnet mask. Use this screen to configure the IPv6 address for the NBG6818 on the LAN. Use this screen to enable the NBG6818's DHCP server.
System	Status	Use this screen to view the basic information of the NBG6818.
	General Setting	Use this screen to change password or to set the timeout period of the management session.
	Maintenance	Use this screen to upload firmware, reboot the NBG6818 without turning the power off or reset the NBG6818 to factory default.
	Operating Mode	Use this screen to select whether your device acts as a router, or a bridge.
	Logs	Use this screen to view the list of activities recorded by your NBG6818.

CHAPTER 6 Standard Mode

6.1 Overview

Use the **Status** screen to view read-only information about your NBG6818 in standard (router) mode.

6.2 Standard Mode Status Screen

Click **Settings** > **System** > **Status** to open the status screen.

Figure 22 Settings > System > Status (Standard Mode)

The following table describes the labels shown in the **Status** screen.

Table 9 Settings > System > Status (Standard Mode)

LABEL	DESCRIPTION
System	
Model Name	This is the model name of your device.
Firmware Version	This is the firmware version.
System Operation Mode	This is the device mode to which the NBG6818 is set, see Section 13.7 on page 141 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the NBG6818.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the NBG6818.
System Uptime	This is the total time the NBG6818 has been on.
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
IP Address	This shows the WAN port's IP address.

Table 9 Settings > System > Status (Standard Mode) (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This shows the WAN port's subnet mask.
Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the current IPv6 address of the NBG6818.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP Server	This shows the LAN port's DHCP role - **Enable** or **Disable**.
IPv6 Address	This shows the current IPv6 address of the NBG6818 in the LAN.

CHAPTER 7
Bridge Mode

7.1 Overview

Many screens that are available in **Standard Mode** are not available in **Bridge Mode**, such as port forwarding and firewall. See Section 5.3 on page 51 for more information.

7.2 What You Can Do

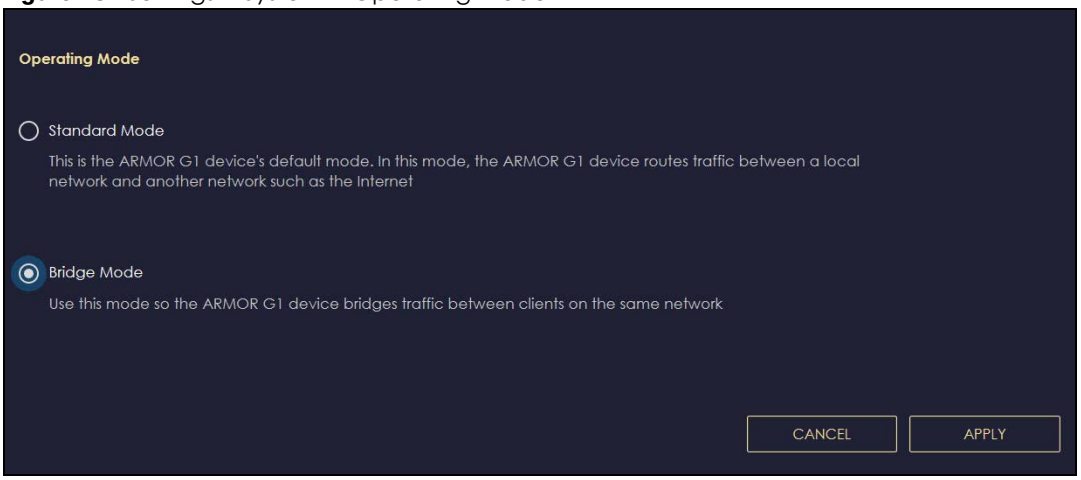
- Set up a network with the NBG6818 as a bridge (Section 7.3 on page 59).
- Use the **Status** screen to view read-only information about your NBG6818 (Section 7.4 on page 60).

7.3 Setting your NBG6818 to Bridge Mode

1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.

2 To use your NBG6818 as a bridge, go to **Settings > System > Operating Mode** and select **Bridge Mode**.

Figure 23 Settings > System > Operating Mode



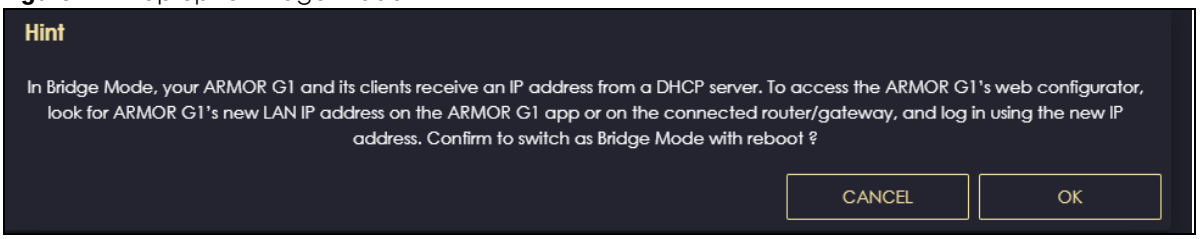
Note: You have to log into the Web Configurator again when you change modes. As soon as you do, your NBG6818 is already in Bridge mode.

Note: Choose your NBG6818 operating mode carefully to avoid having to change it later.

When changing to another mode, the IP address of the NBG6818 changes (192.168.123.1 in standard (router) mode to 192.168.123.2 in bridge mode and vice versa). The running applications and services of the network devices connected to the NBG6818 may be interrupted.

3 When you select **Bridge Mode**, the following pop-up message window appears.

Figure 24 Pop up for Bridge mode



Click **OK**. Then click **Apply**. The Web Configurator refreshes once the change to Bridge mode is successful.

7.3.1 Accessing the Web Configurator in Bridge Mode

Log in to the Web Configurator in Bridge mode, do the following:

1 Log into the Web Configurator. See the Quick Start Guide for instructions on how to do this.

2 Connect your computer to one of the LAN port of the NBG6818.

3 Connect a modem/router to the other LAN port of the NBG6818 using an Ethernet cable.

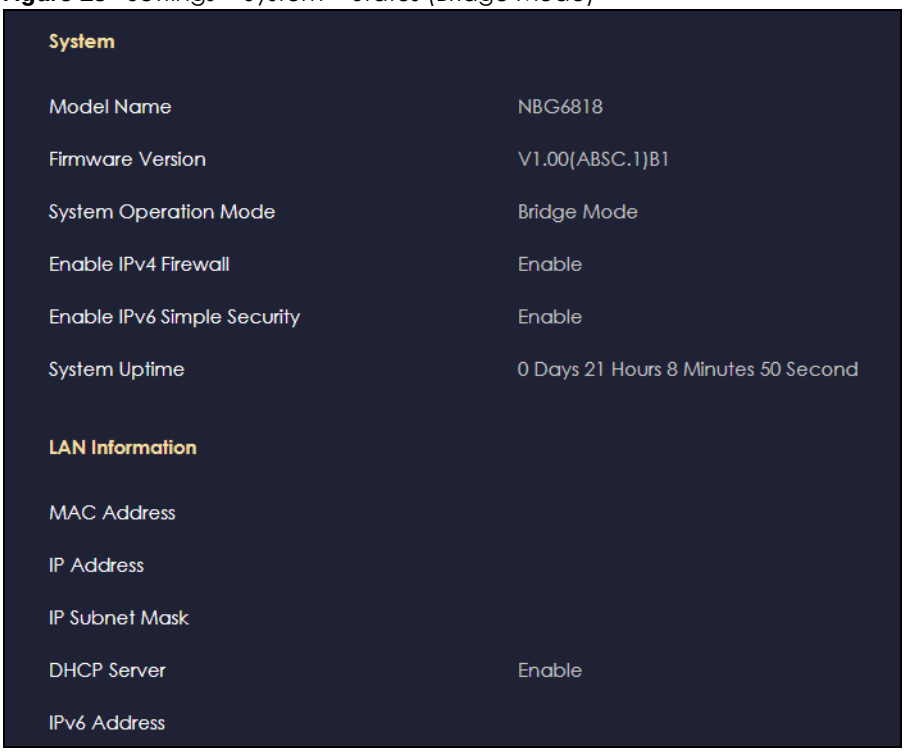
4 If the NBG6818 is not connected to a router or DHCP server, the NBG6818 cannot assign your computer an IP address.

5 After you have set your computer's IP address, open a web browser such as Google Chrome and enter "http://(DHCP-assigned IP)" as the web address in your web browser.

7.4 Bridge Mode Status Screen

Click **Settings** > **System** > **Status** to open the status screen.

Figure 25 Settings > System > Status (Bridge Mode)



The following table describes the labels shown in the **Status** screen.

Table 10 Settings > System > Status (Bridge Mode)

LABEL	DESCRIPTION
System	
Model Name	This is the model name of your device.
Firmware Version	This is the firmware version.
System Operation Mode	This is the device mode to which the NBG6818 is set, see Section 13.7 on page 141 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the NBG6818.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the NBG6818.
System Uptime	This is the total time the NBG6818 has been on.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP Server	This shows the LAN port's DHCP role - **Enable** or **Disable**.
IPv6 Address	This shows the current IPv6 address of the NBG6818 in the LAN.

PART II
Technical Reference

CHAPTER 8 Applications

8.1 Overview

This chapter shows you how to configure parental control, OpenVPN, USB media sharing and file sharing.

8.1.1 What You Can Do

- Use the **Parental Control** screens to enable parental control, configure the parental control rules and schedules, and send e-mail notifications. (Section 8.2 on page 64).
- Use the **OpenVPN Server** screen to create or configure your NBG6818 when it functions as an OpenVPN Server (Section 8.3.1 on page 68).
- Use the **OpenVPN Client** screen to add an OpenVPN Server Account you want your NBG6818 to connect to (Section 8.3.3 on page 71).
- Use the **USB Application** screen to allow file sharing or to set up your NBG6818 to act as a media server (Section 8.4 on page 73).

8.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

DLNA

The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network. DLNA clients play files stored on DLNA servers. The NBG6818 can function as a DLNA-compliant media server and stream files to DLNA-compliant media clients without any configuration.

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file-sharing feature on your NBG6818 supports New Technology File System (NTFS), File Allocation Table (FAT) and FAT32 file systems.

Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

CIFS runs over TCP/IP but uses the SMB (Server Message Block) protocol found in Microsoft Windows for file and printer access; therefore, CIFS will allow all applications, not just Web browsers, to open and share files across the Internet.

The NBG6818 uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the NBG6818. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems.

File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

VPN

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

8.1.3 Before You Begin

Make sure the NBG6818 is connected to your network and turned on.

1. Connect the USB device to one of the NBG6818's USB ports.
2. The NBG6818 detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the NBG6818, see the troubleshooting for suggestions.

8.2 Parental Control

Parental Control allows you to block specific URLs. You can also define time periods and days during which the NBG6818 performs parental control on a specific user.

Note: This is not available if you are using bridge mode.

8.2.1 Device Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Parental Control** > **Device** to show the following screen.

Figure 26 Parental Control > Device

The following table describes the fields in this screen.

Table 11 Parental Control > Device

LABEL	DESCRIPTION
Sort By	Choose to sort the order of your client devices by **Type** or **Name**.
Connect to	Choose whether you want to show client devices that are connected to **Main Network** or devices that are connected **Guest Network**. Choose **All** if you want to show all client devices.
No.	This shows the index number of the rule.
Type	The shows the type of client device to which this rule applies.
Network	This shows the type of network the client devices are connected to.
Name	This shows the name of the user to which this rule applies.
MAC	This field shows the MAC address of the client device with the name in the **Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a client device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
IP Address	This field displays the IP address relative to the **No.** field listed above.
Profile	This shows the name of the rule that is applied to the client device. If no rule exists, **unassigned** is showed in this field.
Action	Click the **Action** icon ( ) to configure a rule for the client device.

8.2.1.1 Edit Device Detail Screen

Use this screen to configure basic settings for the client device. Click the **Action** icon ( ), and then the **Edit** icon ( ) to show the following screen.

Figure 27 Parental Control > Device: Edit

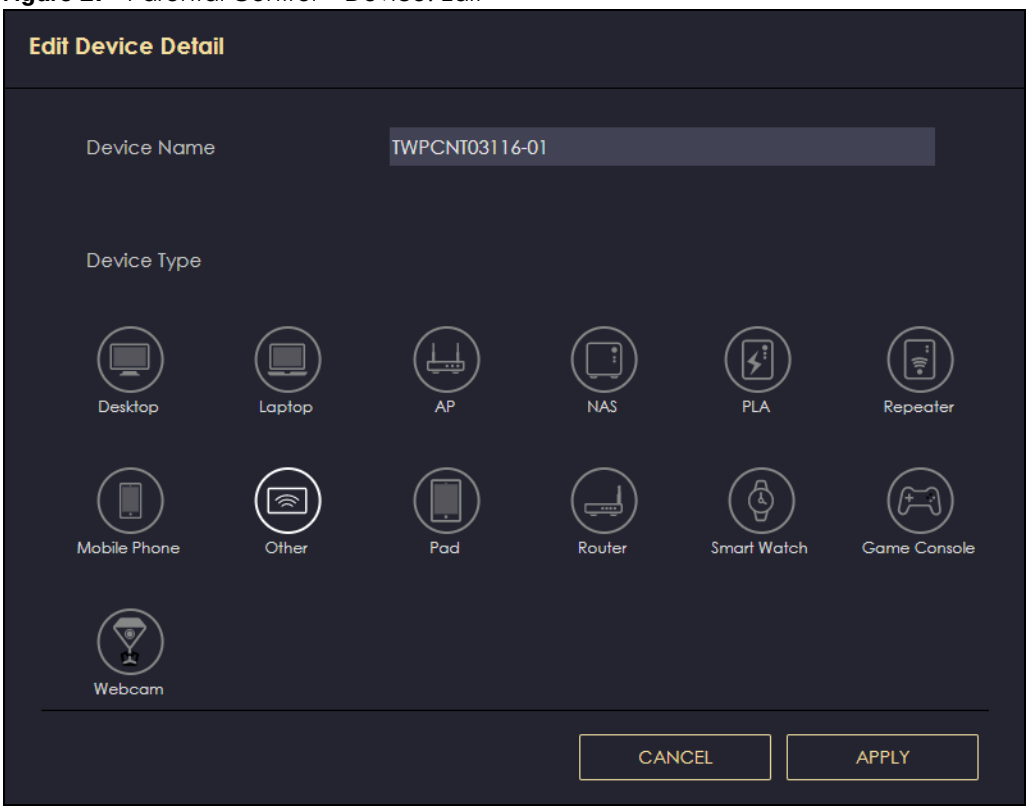


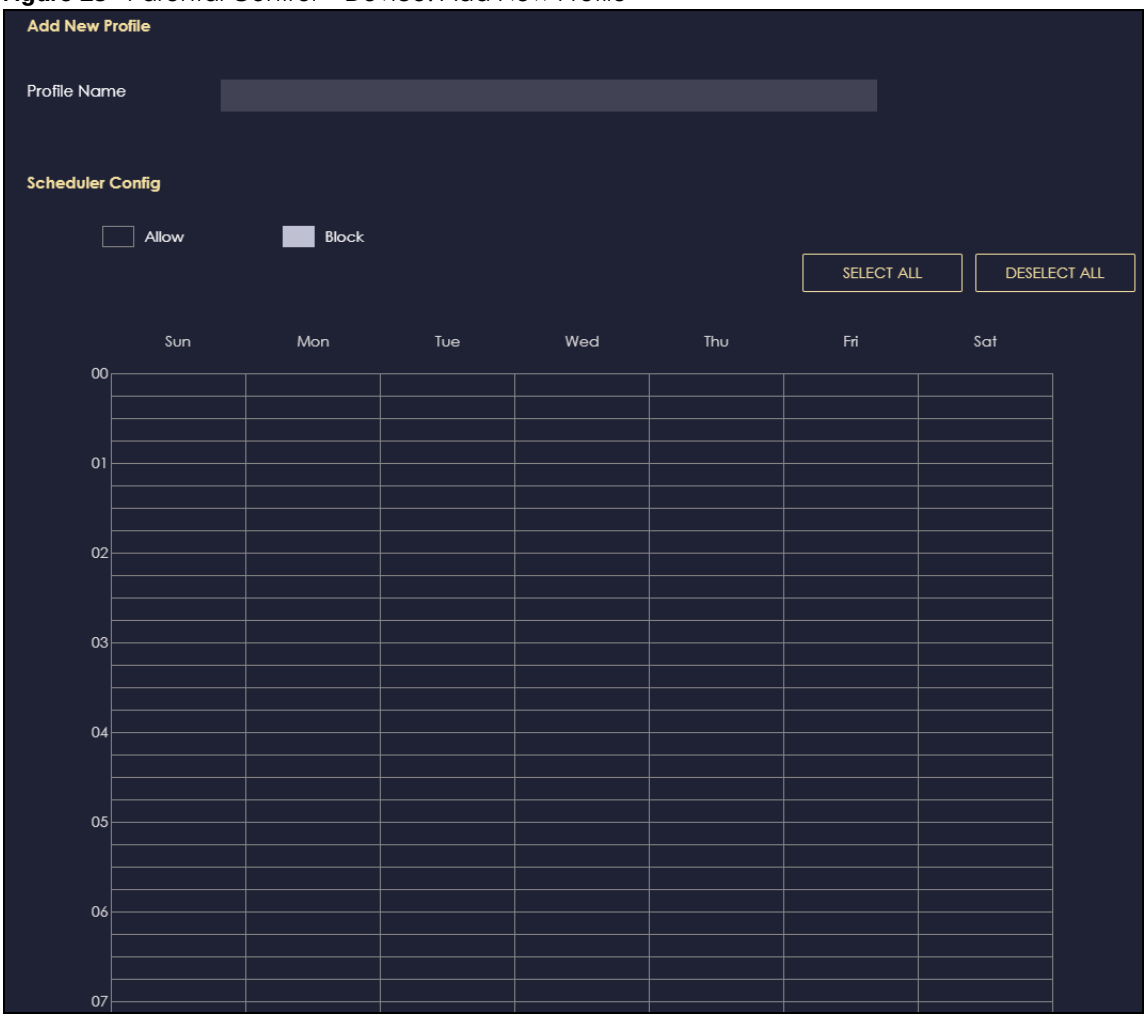
Table 12 Parental Control > Device: Edit

LABEL	DESCRIPTION
Device Name	Enter a name for the device to which this rule applies.
Device Type	Choose the type of device to which this rule applies.
APPLY	Click **APPLY** to save your settings back to the NBG6818.
CANCEL	Click **CANCEL** to exit the screen without saving.

8.2.1.2 Add New Profile Screen

Use this screen to configure a restricted access schedule. Click the **Action** icon ( ), then **Add New Profile** to show the following screen.

Figure 28 Parental Control > Device: Add New Profile



The following table describes the fields in this screen.

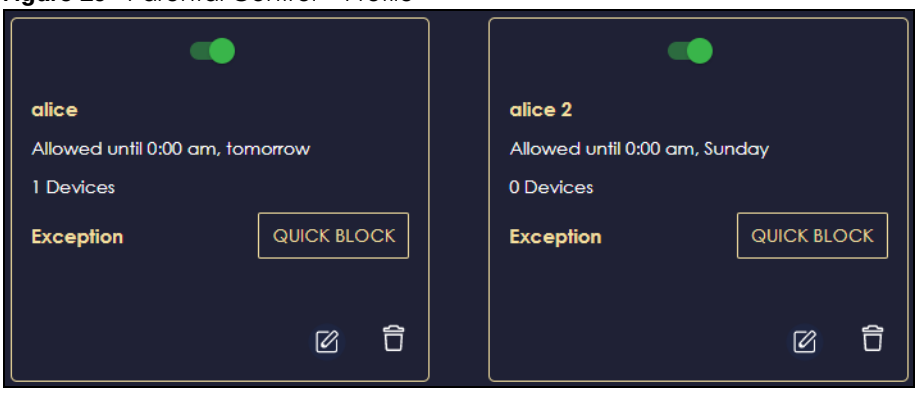
Table 13 Parental Control > Device: Add New Profile

LABEL	DESCRIPTION
Profile Name	Enter a name for this rule.
Scheduler Config	Click **Allow** to select the time slot you allow client devices to access the Internet. Otherwise, click **Block**.
SELECT ALL	Click **SELECT ALL** then deselect the blocks you don't want or click on blocks separately to specify days and times to turn the WiFi on or off.
DESELECTt ALL	Click **DESELECT ALL** to remove all the WiFi scheduling.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
Back	Click **Back** to exit the screen without saving.

8.2.1.3 Profile Screen

Use this screen to edit or delete an existing rule. Click **Parental Control** > **Profile** to show the following screen.

Figure 29 Parental Control > Profile



The following table describes the fields in this screen.

Table 14 Parental Control > Profile

LABEL	DESCRIPTION
Enable/Disable	Set the switch to the right ( ) to enable an existing rule. Otherwise, set the switch to the left ( ).
QUICK BLOCK	Click **QUICK BLOCK** to activate the profile.
Edit	Click on the **Edit** icon to edit an existing rule.
Delete	Click on the **Delete** icon to delete an existing rule.

8.3 OpenVPN Server/Client

Note: We do not recommended activating OpenVPN Server and OpenVPN Client at the same time on your NBG6818.

Note: This is not available if you are using bridge mode.

8.3.1 OpenVPN Server Screen

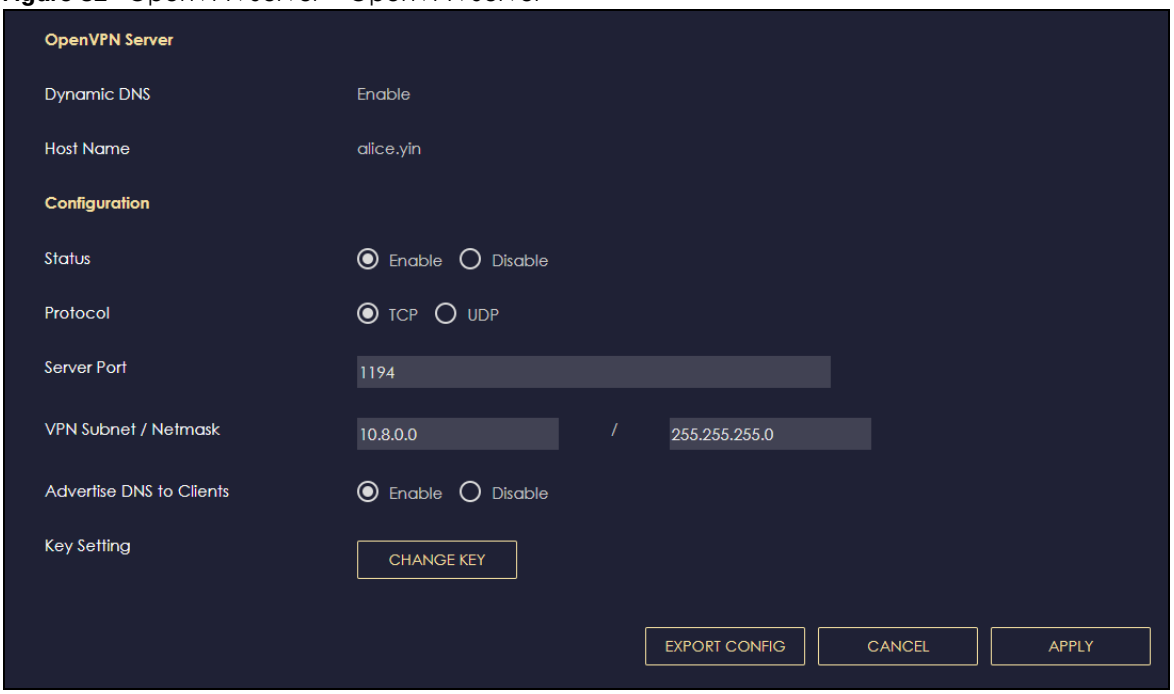
Use this screen to create an OpenVPN server account. Click the **Navigation Panel** icon on the top-left corner ( ). Select **OpenVPN Server**, and click the **OpenVPN Server** tab.

Figure 30 Example of NBG6818 Acting As VPN Server

The NBG6818 (**A**) transmits data through a secure VPN channel (**B**) to the client device (**C**).

You have to enable DDNS in the **Settings** > **Internet** > **Dynamic DNS** screen before you can create an OpenVPN account. See Section 9.8 on page 102 for more information on Dynamic DNS.

Figure 31 OpenVPN Server > OpenVPN Server



The following table describes the fields in this screen.

Table 15 OpenVPN Server > OpenVPN Server

LABEL	DESCRIPTION
OpenVPN Server	
Dynamic DNS	This field shows the status of your Dynamic DNS. Make sure it shows **Enable** before you create an OpenVPN account.
Host Name	This field shows the Host Name of your Dynamic DNS account.
Configuration	
Status	Select **Enable** to activate your OpenVPN Server account.
Protocol	Select the protocol you want to apply to your OpenVPN Server account.
Server Port	The default server port number is 1194. You can change it if needed. However, clients connected to this OpenVPN Server account will have to use the same port number in order to access the server account.
VPN Subnet/ Netmask	The fields define the network from which OpenVPN clients can connect to the NBG6818 OpenVPN server. Enter an IPv4 address and subnet mask.
Advertise DNS to Clients	Select **Enable** if you want the NBG6818 to broadcast its OpenVPN server to OpenVPN clients in its VPN network defined previously.
Key Setting	Click the **CHANGE KEY** button if you want to change the key your clients use to access to your OpenVPN Server account. You do not need to click **CHANGE KEY** the first time to configure this screen. Periodically changing the key is recommended, but you must export the new .opvn configuration file and send it to all OpenVPN clients so that they can use the new key.

Table 15 OpenVPN Server > OpenVPN Server (continued)

LABEL	DESCRIPTION
EXPORT CONFIG	Click **EXPORT CONFIG** to export your configuration to an .ovpn file that OpenVPN clients need to connect to the NBG6818 OpenVPN server.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

8.3.2 OpenVPN Account Screen

Use the **OpenVPN Account List** screen to view the basic information of the NBG6818 OpenVPN server.

Use the **OpenVPN Account Status** screen to view the basic information of clients that are connected to the NBG6818 OpenVPN server.

Note: At the time of writing, up to 16 OpenVPN clients can connect to the NBG6818 OpenVPN server at the same time.

Figure 32 OpenVPN Server > OpenVPN Account

The following table describes the fields in this screen.

Table 16 Open VPN Server > Open VPN Account

LABEL	DESCRIPTION
OpenVPN Account List	
No.	This is the rule index number.
Username	This field displays a name to identify this rule.
Password	This field displays a combination of characters and numbers clients need to connect to an account.
Client Access Allowed	This field displays the interface(s) through which the clients are allowed to connect to an account.
Actions	Click the icons under **Actions** to delete or edit an existing OpenVPN account settings. Click to delete an existing OpenVPN account. Click to edit an existing OpenVPN account.
OpenVPN Account Status	
No.	This is the number used to identify a client.

Table 16 Open VPN Server > Open VPN Account

LABEL	DESCRIPTION
Public IP	This field displays the public IP of a client.
Private IP	This field displays the private IP of a client.
Connected Time	This field displays how long a client is connected.

8.3.2.1 OpenVPN Account List-Add Rule Screen

Use this screen to configure your OpenVPN account settings.

Figure 33 Open VPN Server > Open VPN Account: Add Rule

The following table describes the fields in this screen.

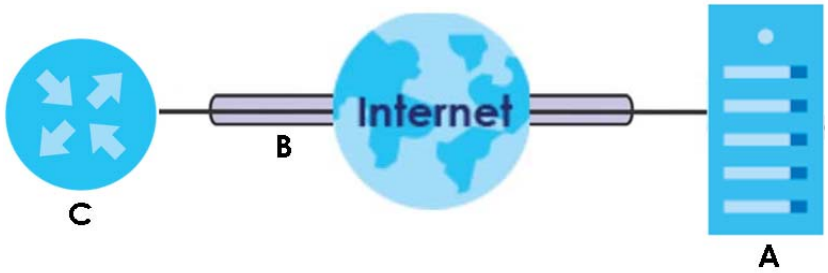
Table 17 Open VPN Server > Open VPN Account: Add Rule

LABEL	DESCRIPTION
User Name	Enter 1-32 single-byte printable ASCII characters, but <>^$& are not allowed.
Password	Enter 1-32 single-byte printable ASCII characters, but <>^$& are not allowed.
Client Access Allowed	Select the interface(s) through which the clients are allowed to connect to your account.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to exit this screen without saving.

8.3.3 OpenVPN Client Screen

Use the **OpenVPN Server List** in this screen to view the basic information of the OpenVPN Server accounts that you are connected to when the NBG6818 functions as an OpenVPN client.

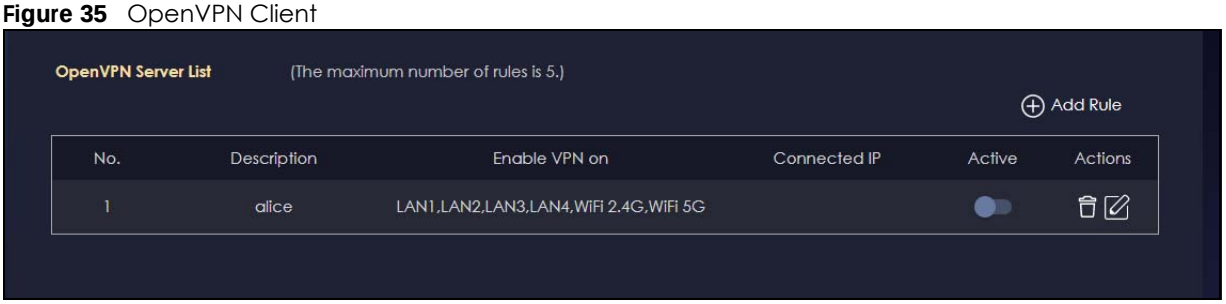
Figure 34 Example of NBG6818 Acting As VPN Client



The VPN server (**A**) transmits data through a secure VPN channel (**B**) to the NBG6818 (**C**) client device.

Note: You can only connect to one server at a time.

Figure 35 OpenVPN Client



The following table describes the fields in this screen.

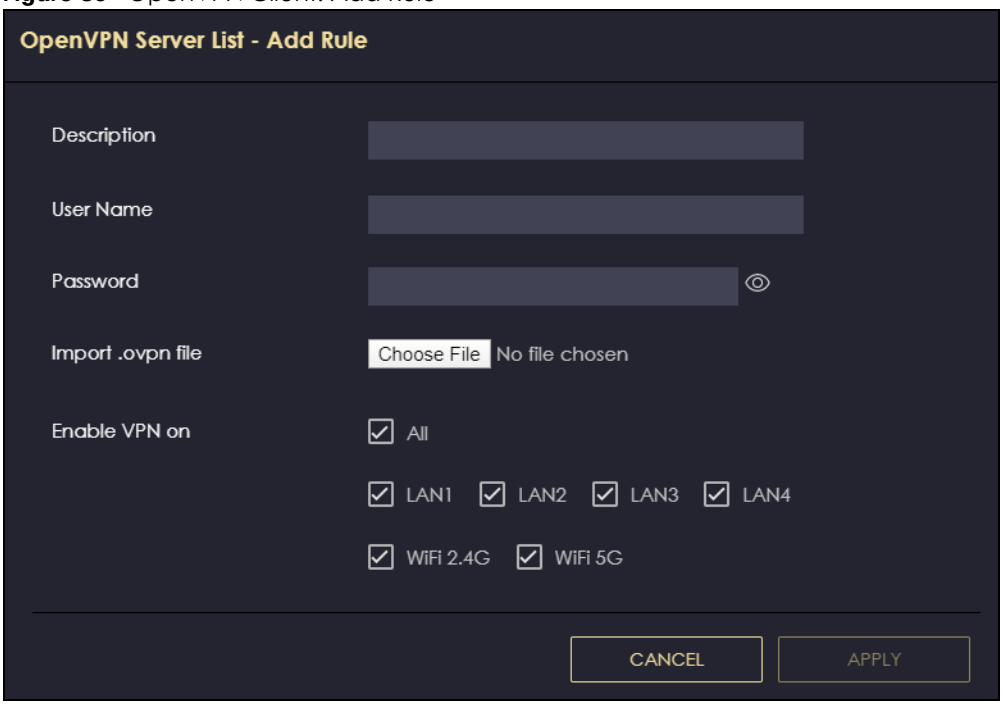
Table 18 OpenVPN Client

LABEL	DESCRIPTION
No.	This is the rule index number.
Description	This field displays a name to identify this rule.
Enable VPN on	This field displays the interface(s) through which your NBG6818 are allowed to connect to an OpenVPN Server account.
Connected IP	This field displays the IP address of the OpenVPN Server account your NBG6818 is connected to.
Active	Slide the switch to the right ( ) to activate your connection to an OpenVPN Server account.
Actions	Click the icons under **Actions** to delete or edit an existing OpenVPN Server account settings. Click to delete an existing OpenVPN Server account. Click to edit an existing OpenVPN Server account.

8.3.3.1 OpenVPN Server List-Add Rule Screen

Use this screen to add an OpenVPN Server Account that you want your NBG6818 to connect to.

Figure 36 OpenVPN Client: Add Rule



The following table describes the fields in this screen.

Table 19 OpenVPN Client: Add Rule

LABEL	DESCRIPTION
Description	Enter 1-32 single-byte printable ASCII characters, but <>^$& are not allowed.
User Name	Enter the **User Name** of the OpenVPN Server account you want to connect to.
Password	Enter the **Password** of the OpenVPN Server account you want to connect to.
Import .ovpn file	Import an .ovpn file that you get from the OpenVPN Server that you want to connect to. Note: Do not import the .ovpn file you get from your NBG6818's OpenVPN Server.
Enable VPN on	Select the interface(s) that are allowed by the OpenVPN Server account you want to connect to.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to exit this screen without saving.

8.4 USB Application

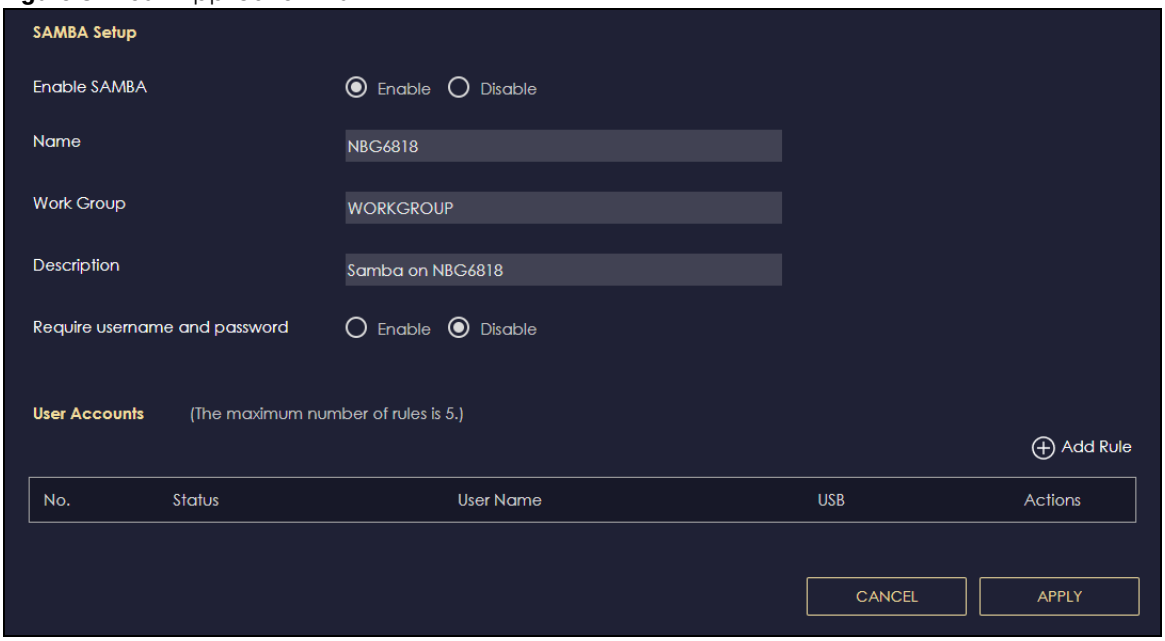
Configure file sharing through File Explorer / FTP with users on your network using a USB memory stick or hard drive connected to your NBG6818. You can also configure your NBG6818 to function as a DLNA-compliant media server.

8.4.1 SAMBA Server Screen

Use this screen to set up file-sharing via the NBG6818 using Windows Explorer or the workgroup name. You can also configure the workgroup name and create file-sharing user accounts.

Click **USB Application > SAMBA** to show the following screen.

Figure 37 USB Application > SAMBA



The following table describes the labels in this screen.

Table 20 USB Application > SAMBA

LABEL	DESCRIPTION
SAMBA Setup	
Enable SAMBA	Select this to enable file sharing through the NBG6818 using Windows Explorer or by browsing to your work group.
Name	Specify the name to identify the NBG6818 in a work group.
Work Group	You can add the NBG6818 to an existing or a new workgroup on your network. Enter the name of the workgroup which your NBG6818 automatically joins. You can set the NBG6818's workgroup name to be exactly the same as the workgroup name to which your computer belongs to. Note: The NBG6818 will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.
Description	Enter the description of the NBG6818 in a work group.
Require username and password	Select **Yes** to need a user account for access to the connected USB stick from any computer. Otherwise, select **No**.
User Accounts	Before you can share files you need a user account. Configure the following fields to set up a file-sharing account.
No.	This is the index number of the user account.
Status	This field displays whether a user account is activated or not.
User Name	This field displays the user name that will be allowed to access the shared files.

Table 20 USB Application > SAMBA (continued)

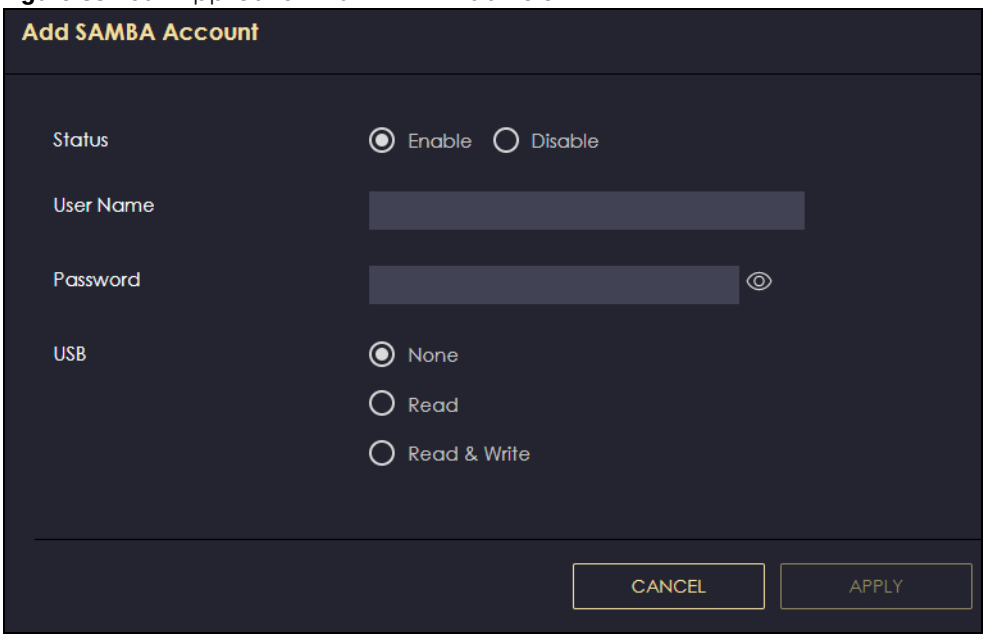
LABEL	DESCRIPTION
USB	This field displays the user's access rights to the USB storage device which is connected to the NBG6818's USB port.
Actions	Click the icons under **Actions** to delete or edit a port forwarding rule. Click to delete an existing trigger port settings. Click to edit an existing trigger port settings.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

8.4.1.1 Add SAMBA Account Screen

Use this screen to configure settings for a SAMBA account.

Click **USB Application** > **SAMBA** > **Add Rule** to show the following screen.

Figure 38 USB Application > SAMBA > Add Rule



The following table describes the labels in this screen.

Table 21 USB Application > SAMBA > Add Rule

LABEL	DESCRIPTION
Status	Select **Enable** to enable the account. Select **Disable** to disable the account.
User Name	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.

Table 21 USB Application > SAMBA > Add Rule

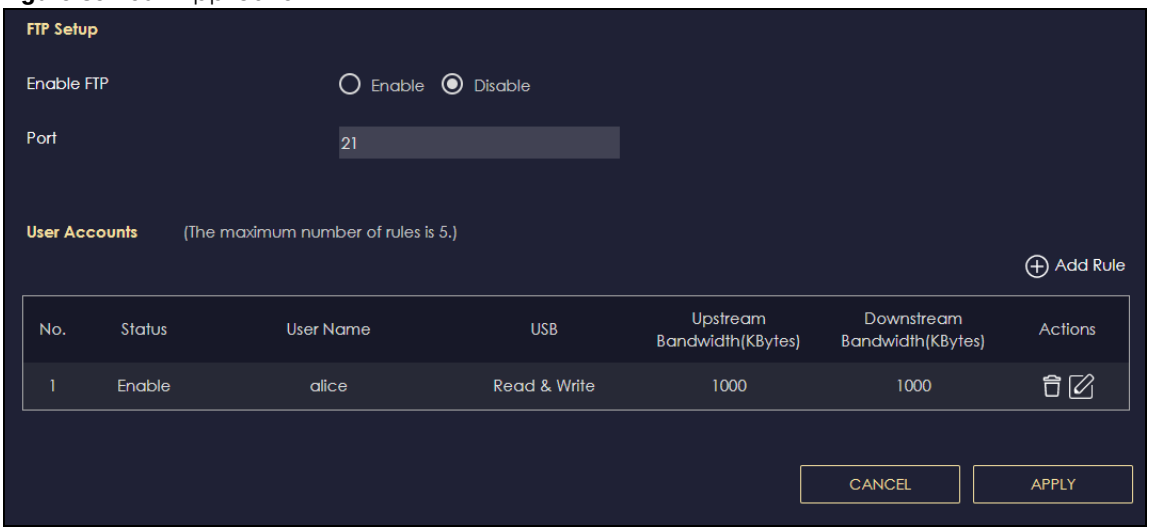
LABEL	DESCRIPTION
USB	Specify the user's access rights to the USB storage device which is connected to the NBG6818's USB port. **Read & Write** - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. **Read** - The user has read rights only and can not create or edit the files on the connected USB device. **None** - The user cannot access the files on the USB device(s) connected to the USB port.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to exit the screen without saving.

8.4.2 FTP Server Screen

Use this screen to set up file sharing via the NBG6818 using FTP and create user accounts.

Click **USB Application** > **FTP** to show the following screen.

Figure 39 USB Application > FTP



The following table describes the labels in this screen.

Table 22 USB Application > FTP

LABEL	DESCRIPTION
Enable FTP	Select this to enable the FTP server on the NBG6818 for file sharing using FTP.
Port	You may change the server port number for FTP if needed, however you must use the same port number in order to use that service for file sharing.
User Accounts	Before you can share files you need a user account. Configure the following fields to set up a file-sharing account.
No.	This is the index number of the user account.
Status	This field displays whether a user account is activated or not. Select the check box to enable the account. Clear the check box to disable the account.
User Name	This field displays the user name that will be allowed to access the shared files.

Table 22 USB Application > FTP (continued)

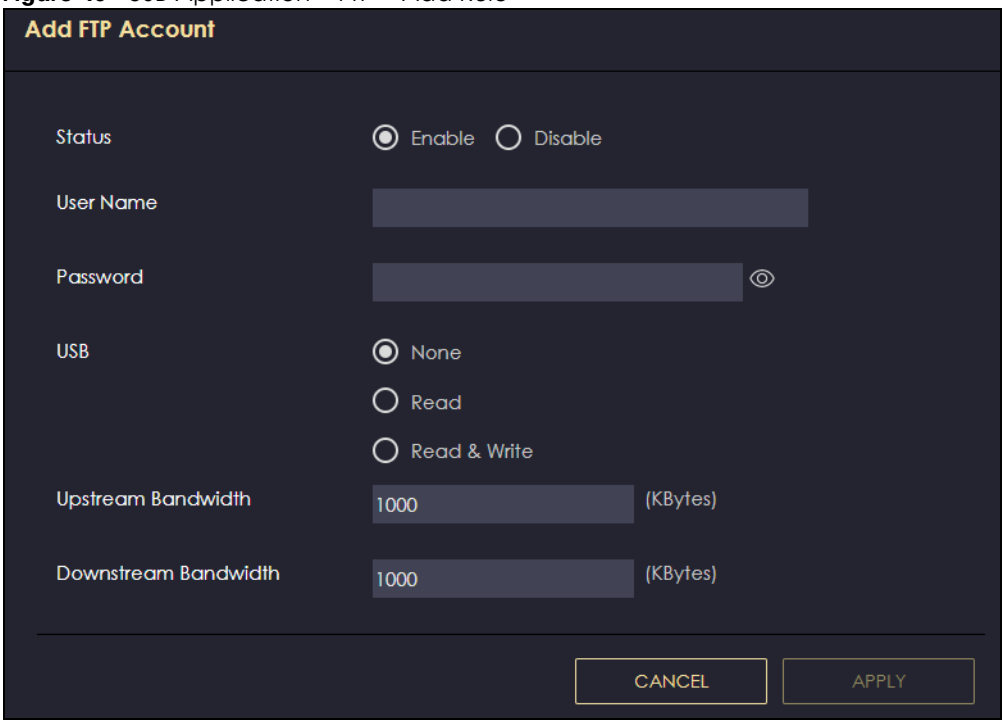
LABEL	DESCRIPTION
USB	This field displays the user's access rights to the USB storage device which is connected to the NBG6818's USB port.
Upstream Bandwidth	This field shows the maximum bandwidth (in Kbps) allowed for incoming FTP traffic.
Downstream Bandwidth	This field shows the maximum bandwidth (in Kbps) allowed for outgoing FTP traffic.
Actions	Click the icons under **Actions** to delete or edit a port forwarding rule. Click to delete an existing trigger port settings. Click to edit an existing trigger port settings.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

8.4.2.1 Add FTP Account Screen

Use this screen to configure settings for a FTP account.

Click **USB Application** > **FTP** > **Add Rule** to show the following screen.

Figure 40 USB Application > FTP > Add Rule



The following table describes the labels in this screen.

Table 23 USB Application > FTP > Add Rule

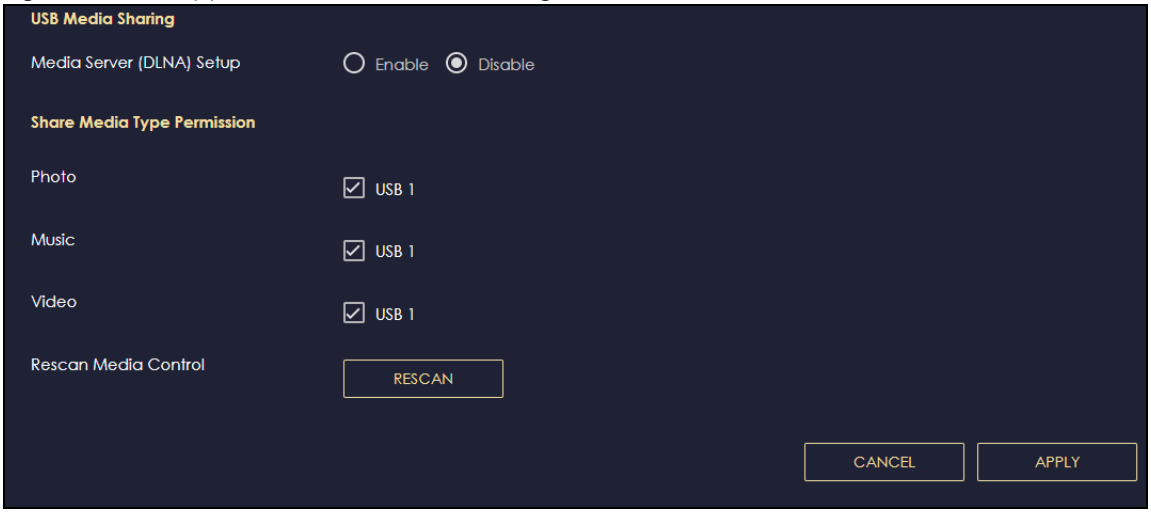
LABEL	DESCRIPTION
Status	Select **Enable** to enable the account. Select **Disable** to disable the account.
User Name	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.
USB	Specify the user's access rights to the USB storage device which is connected to the NBG6818's USB port. **Read & Write** - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. **Read** - The user has read rights only and can not create or edit the files on the connected USB device. **None** - The user cannot access the files on the USB device(s) connected to the USB port.
Upstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for incoming FTP traffic.
Downstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for outgoing FTP traffic.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to exit the screen without saving.

8.4.3 USB Media Sharing Screen

Use this screen to configure settings for media sharing.

Click **USB Application** > **USB Media Sharing** to show the following screen.

Figure 41 USB Application > USB Media Sharing



The following table describes the labels in this screen.

Table 24 USB Application > USB Media Sharing

LABEL	DESCRIPTION
USB Media Sharing	
Media Server (DLNA) Setup	Choose **Enable** to have the NBG6818 function as a DLNA-compliant media server. Otherwise, choose **Disable**.
Share Media Type Permission	
Photo/Music/Video	Select the media type that you want to share on the USB device connected to the NBG6818's USB port.
Rescan Media Control	
RESCAN	Click this button to have the NBG6818 scan the media files on the connected USB device and do indexing of the file list again so that DLNA clients can find the new files if any.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

8.5 Access Your Shared Files From a Computer

This section shows you how to access shared files from a computer using File Explorer or through FTP.

8.5.1 Using File Explorer

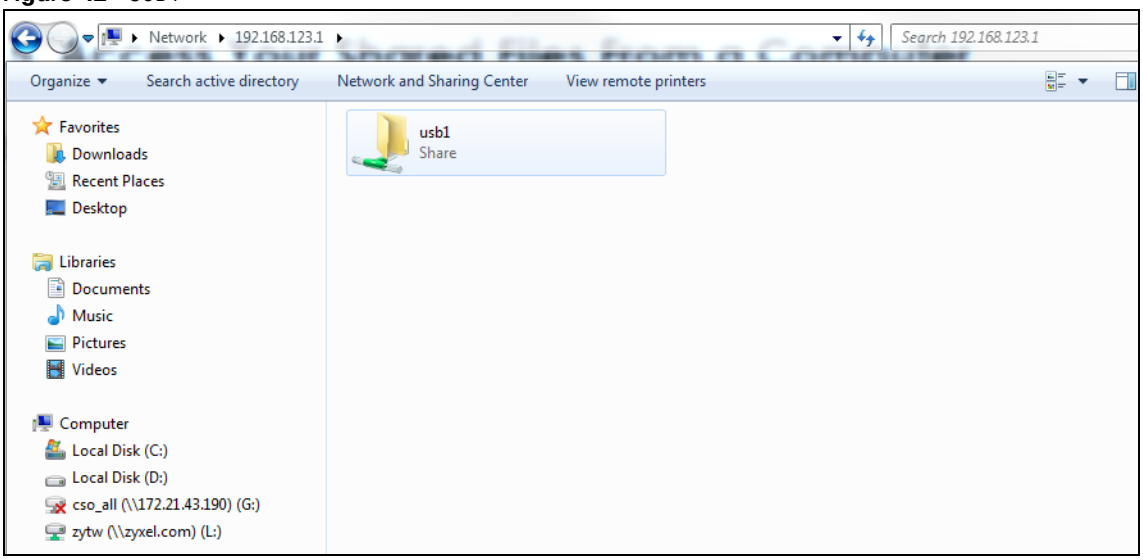
You can use Windows Explorer to access the file storage devices connected to the NBG6818.

Note: The examples in this User's Guide show you how to use Microsoft's Windows 10 to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Open Windows Explorer to access **usb1** using the Windows Explorer browser.

In the Windows Explorer's address bar enter a double backslash "\\" followed by the IP address of the NBG6818 (the default IP address of the NBG6818 is 192.168.123.1) and press [ENTER]. The share folder **usb1** is available.

Figure 42 USB1



Once you access **usb1** via your NBG6818, you do not have to relogin unless you restart your computer.

8.5.2 Using an FTP Program

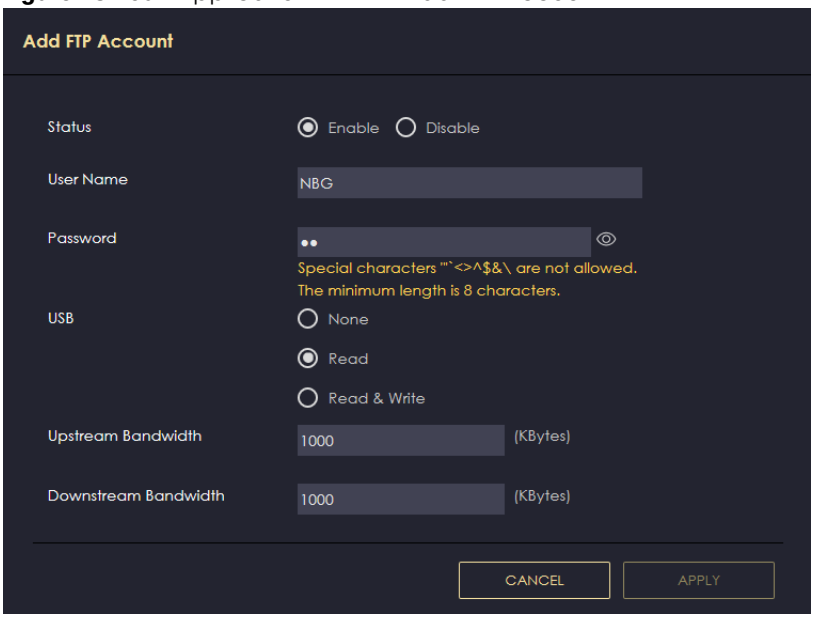
Here is how to use an FTP program to access a file storage device connected to the NBG6818's USB port.

Note: This example uses the FileZilla FTP program to browse your shared files.

1 Download FileZilla and install the FTP software to your computer

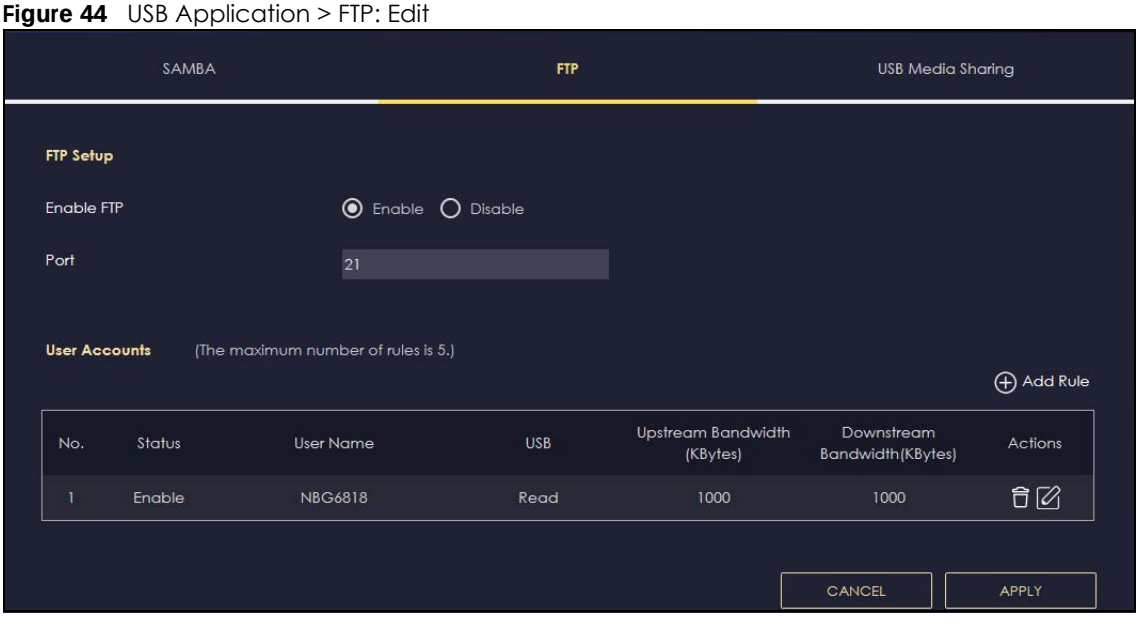
2 Go to **USB Application** > **FTP**. In the **FTP Setup** screen, click **Add Rule** to go to the **Add FTP Account** screen. You can use this screen to create a set of **User Name** and **Password** and set up USB rules for file sharing. (See more information at Section 8.4.2 on page 76.) Click **APPLY** to save the changes.

Figure 43 USB Application > FTP > Add FTP Account



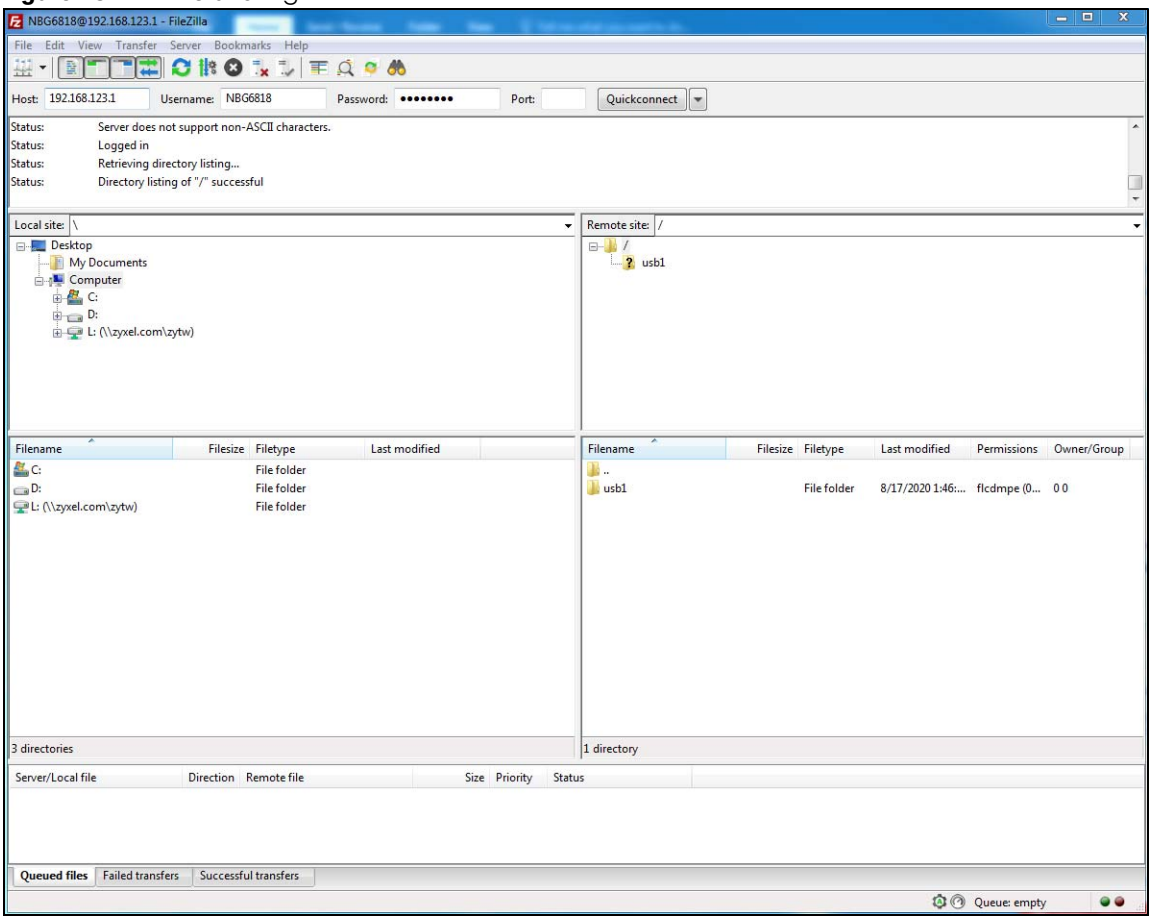
3 You can click the **Edit** or **Delete** icon to edit or delete the rules.

Figure 44 USB Application > FTP: Edit



4 Open FileZilla, enter the **Host** IP address of the NBG6818 (the default IP address is 192.168.123.1), the **Username** and **Password**, and the **port** number 21, and then click **Quickconnect**. A screen asking for password authentication appears.

Figure 45 FTP File Sharing



5 Once you log in, the USB device displays in the **usb1** folder.

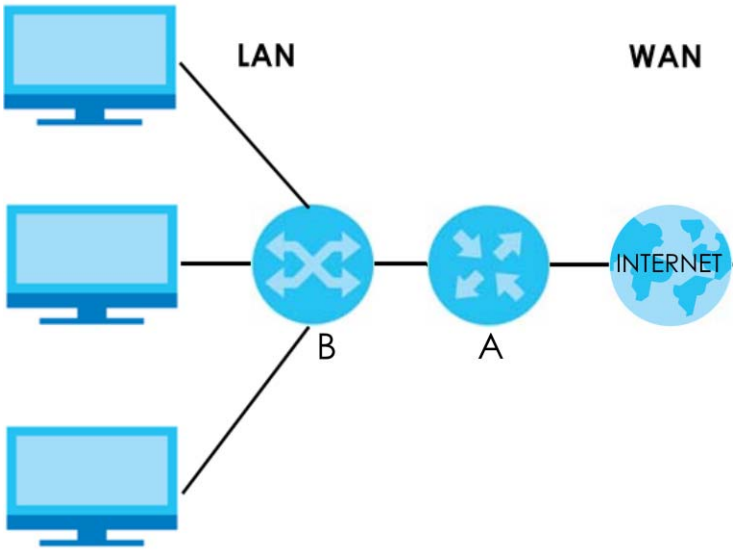
CHAPTER 9
WAN

9.1 Overview

This chapter discusses the NBG6818's **WAN** screens. Use these screens to configure your NBG6818 for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers through a Switch (**B**) in other locations through the NBG6818 (**A**).

Figure 46 LAN and WAN



Note: Features in this chapter are not available if you are using bridge mode.

9.2 What You Can Do

- Use the **Internet Connection** screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses (Section 9.4 on page 86).
- Use the **NAT & Port Forwarding** screen to enable NAT, set a default server and change your NBG6818's port forwarding settings (Section 9.5 on page 94).
- Use the **Passthrough** screen to configure your NBG6818's ALGs and VPN pass-through settings (Section 9.6 on page 98).
- Use the **Port Trigger** screen to configure your NBG6818's trigger port settings (Section 9.7 on page 99).
- Use the **Dynamic DNS** screen to change your NBG6818's DDNS settings (Section 9.8 on page 102).

- Use the **UPnP** screen to enable UPnP on your NBG6818 (Section 9.9 on page 103).

9.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your NBG6818.

9.3.1 Configuring Your Internet Connection

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPTP (Point-to-Point Tunneling Protocol), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the NBG6818, which makes it accessible from an outside network. It is used by the NBG6818 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG6818 tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The NBG6818 can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the NBG6818's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be

copied to configuration file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

IPv6 Subnet Masking

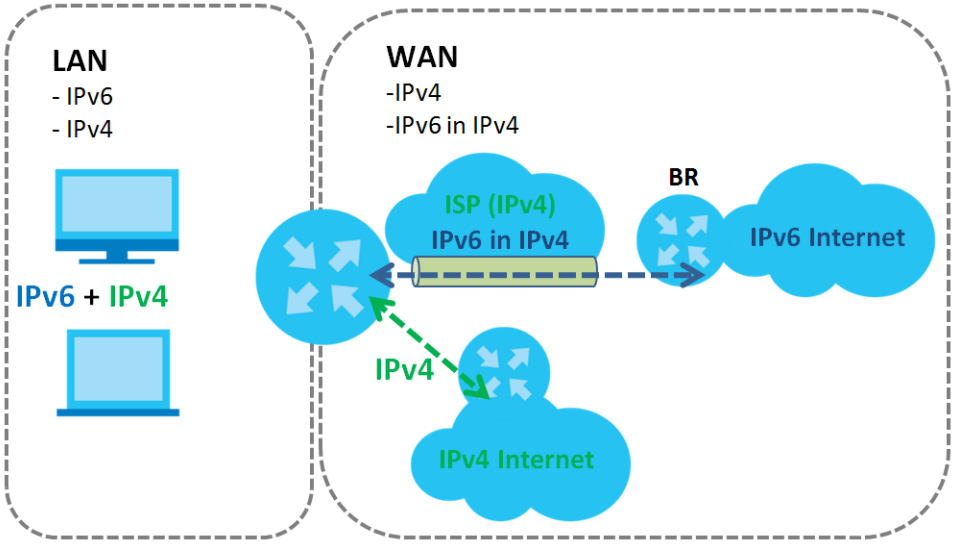
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the NBG6818 has an IPv4 WAN address and you set **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The NBG6818 generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The NBG6818 uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 47 IPv6 Rapid Deployment



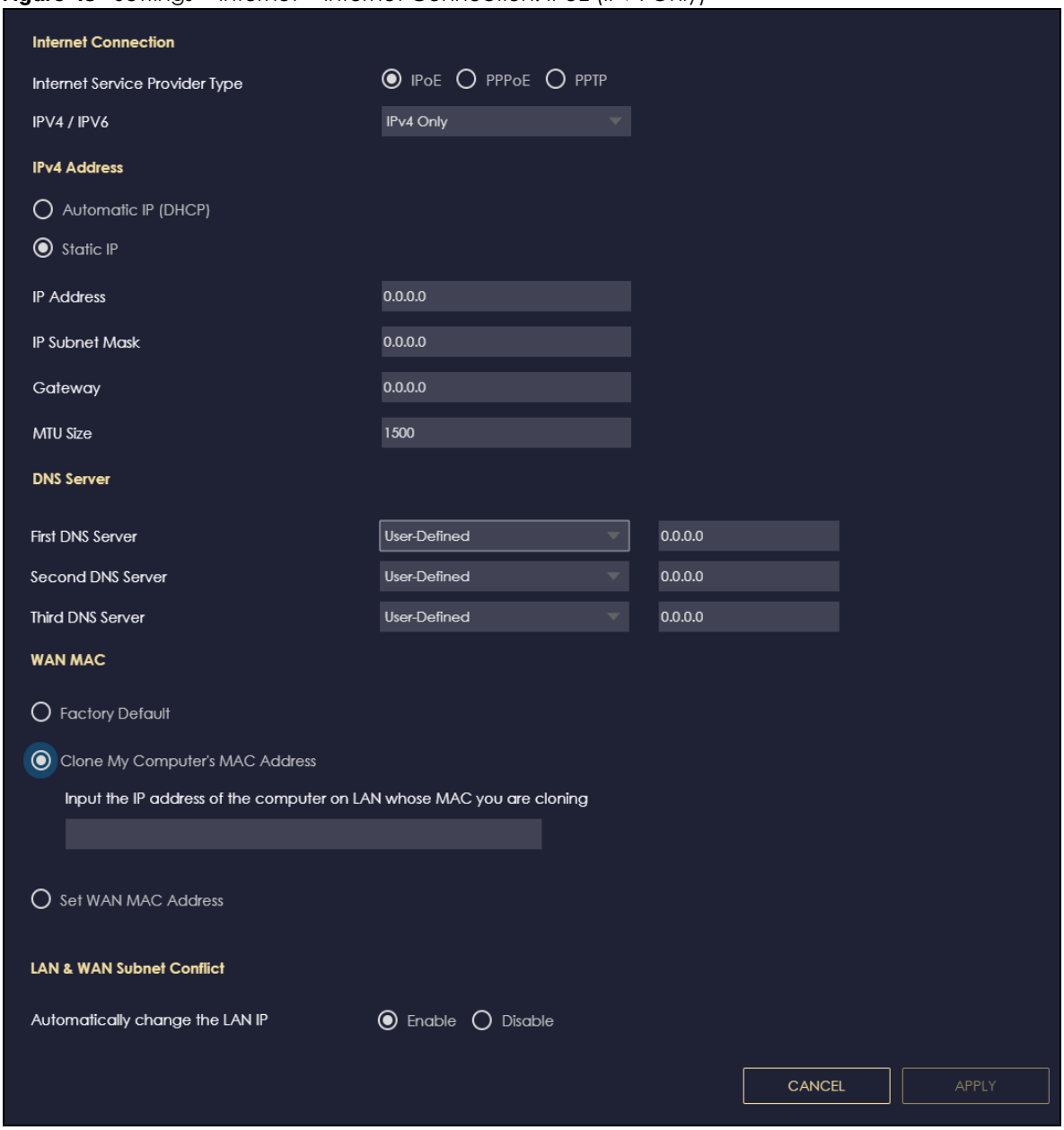
9.4 Internet Connection Screen

Use this screen to change your NBG6818's Internet access settings. The screen varies depending on the encapsulation method you select. Click **Settings** > **Internet** > **Internet Connection**.

9.4.1 IPoE Encapsulation

This screen displays when you select **IPoE** encapsulation.

Figure 48 Settings > Internet > Internet Connection: IPoE (IPv4 Only)



The following table describes the labels in this screen.

Table 25 Settings > Internet > Internet Connection: IPoE

LABEL	DESCRIPTION
Internet Connection	
Internet Service Provider Type	You must choose the **IPoE** option when the WAN port is used as a regular Ethernet.
IPv4 / IPv6	Select **IPv4 Only** if you want the NBG6818 to run IPv4 only. Select **Dual Stack** to allow the NBG6818 to run IPv4 and IPv6 at the same time.
IPv4 Address	
Automatic IP (DHCP)	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.

Table 25 Settings > Internet > Internet Connection: IPoE (continued)

LABEL	DESCRIPTION
Static IP	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Static IP Address**.
IP Subnet Mask	Enter the **Subnet Mask** in this field.
Gateway	Enter a gateway IP address (if your ISP gave you one) in this field.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the NBG6818 divides it into smaller fragments.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address Once the WAN MAC address is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.	
Factory Default	Select this option to have the WAN interface use the factory assigned default MAC address. By default, the NBG6818 uses the factory assigned MAC address to identify itself.
Clone My Computer's MAC Address	Select this option to have the WAN interface use a different MAC address by cloning the MAC address of another device or computer. Enter the IP address of the device or computer whose MAC you are cloning.
Set WAN MAC Address	Select this option to have the WAN interface use a manually specified MAC address. Enter the MAC address in the fields.
LAN & WAN Subnet Conflict	
Automatically change the LAN IP	Select this option to have the NBG6818 change its LAN IP address to 10.0.0.1 or 192.168.123.1 accordingly when the NBG6818 gets a dynamic WAN IP address in the same subnet as the LAN IP address. See Section 9.3.1 on page 84 for more information. The NAT, DHCP server and firewall functions on the NBG6818 are still available in this mode.
IPv6 Address This section is NOT available when you select **IPv4 Only** in the **IPv4/IPv6** field.	
Automatic IP (DHCP)	Select this option if you want to obtain an IPv6 address from a DHCPv6 server. • Select **DUID-LL (Default)** to have the NBG6818 use DUID-LL (DUID Based on Link-layer Address) for identification when exchanging DHCPv6 messages. • Select **DUID-LLT** to have the NBG6818 use DUID-LLT (DUID Based on Link-layer Address Plus Time) for identification when exchanging DHCPv6 messages.
Static IP Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the IPv6 address assigned by your ISP.
Prefix length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Gateway	Enter the IPv6 address of the next-hop gateway. The gateway helps forward packets to their destinations.
Link Local Only	Select this option to use the link-local address which uniquely identifies a device on the local network (the LAN).
IPv6 DNS Server This section is NOT available when you select **IPv4 Only** in the **IPv4/IPv6** field.	

Table 25 Settings > Internet > Internet Connection: IPoE (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** and enter the IPv6 DNS server address assigned by the ISP to have the NBG6818 use the IPv6 DNS server addresses you configure manually. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IPv6 address of a computer in order to access it.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

9.4.2 PPPoE Encapsulation

The NBG6818 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius).

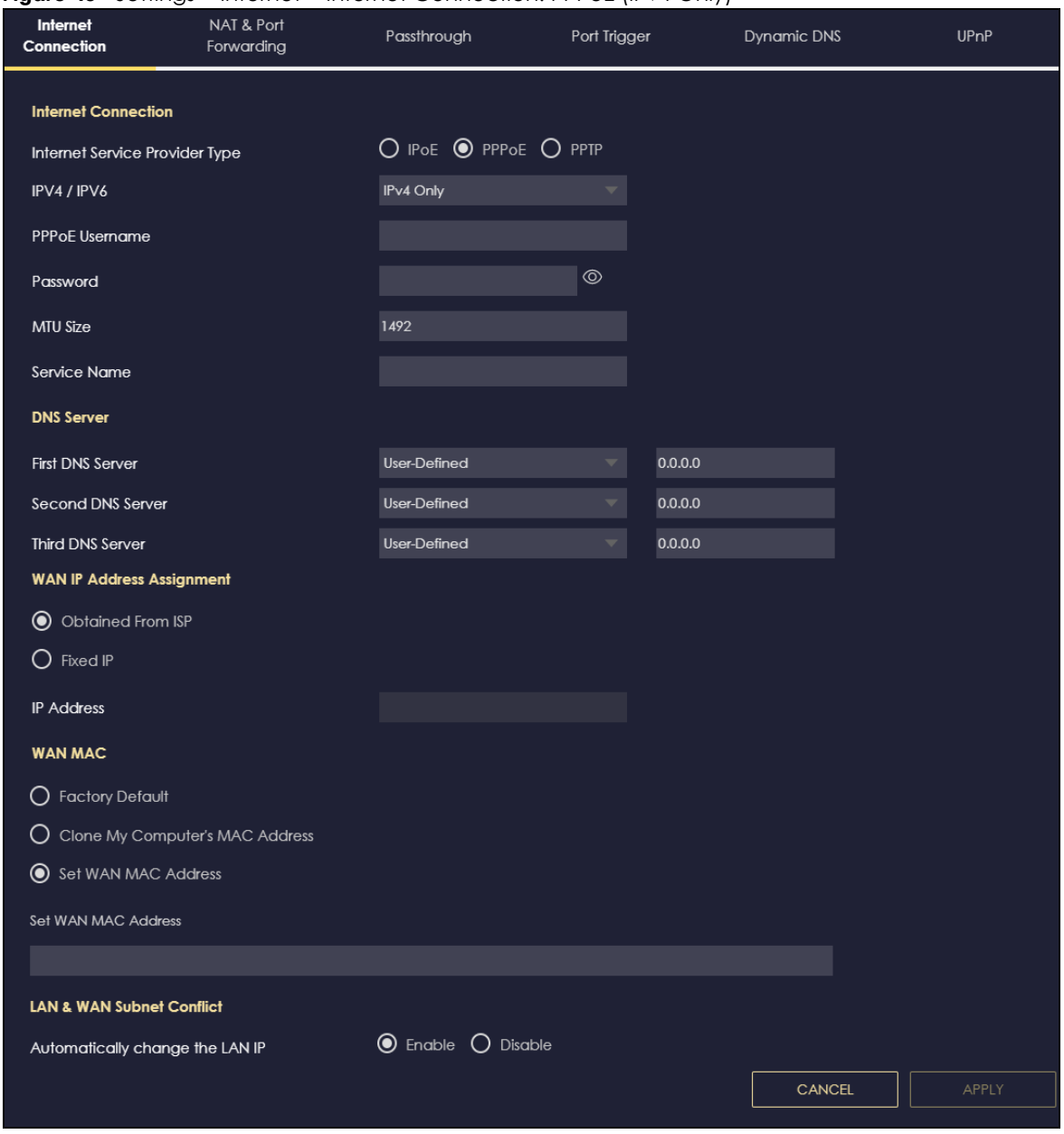
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the NBG6818 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG6818 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select **PPPoE** encapsulation.

Figure 49 Settings > Internet > Internet Connection: PPPoE (IPv4 Only)



The following table describes the labels in this screen.

Table 26 Settings > Internet > Internet Connection: PPPoE

LABEL	DESCRIPTION
Internet Connection	
Internet Service Provider Type	Select **PPPoE** if you connect to your Internet via dial-up.
IPv4 / IPv6	Select **IPv4 Only** if you want the NBG6818 to run IPv4 only. Select **Dual Stack** to allow the NBG6818 to run IPv4 and IPv6 at the same time.
PPPoE Username	Enter the user name given to you by your ISP.

Table 26 Settings > Internet > Internet Connection: PPPoE

LABEL	DESCRIPTION
Password	Enter the password associated with the user name above.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your NBG6818 can receive and process.
Service Name	Enter the PPPoE service name specified in the ISP account.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN IP Address Assignment	
Obtained from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Fixed IP	Select this option and enter your WAN IP address if the ISP assigned a fixed IP address.
WAN MAC Address The MAC address section allows users to configure the WAN port's MAC address by using the NBG6818's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.	
Factory Default	Select **Factory default** to use the factory assigned default MAC Address.
Clone My Computer's MAC Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
IPv6 Address This section is NOT available when you select **IPv4 Only** in the **IPv4/IPv6** field.	
Automatic IP (DHCP)	Select this option if you want to obtain an IPv6 address from a DHCPv6 server. • Select **DUID-LL (Default)** to have the NBG6818 use DUID-LL (DUID Based on Link-layer Address) for identification when exchanging DHCPv6 messages. • Select **DUID-LLT** to have the NBG6818 use DUID-LLT (DUID Based on Link-layer Address Plus Time) for identification when exchanging DHCPv6 messages.
Static IP Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the IPv6 address assigned by your ISP.
Prefix length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Gateway	Enter the IPv6 address of the next-hop gateway. The gateway helps forward packets to their destinations.
Link Local Only	Select this option to use the link-local address which uniquely identifies a device on the local network (the LAN).
IPv6 DNS Server This section is NOT available when you select **IPv4 Only** in the **IPv4/IPv6** field.	
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** and enter the IPv6 DNS server address assigned by the ISP to have the NBG6818 use the IPv6 DNS server addresses you configure manually. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IPv6 address of a computer in order to access it.
LAN & WAN Subnet Conflict	

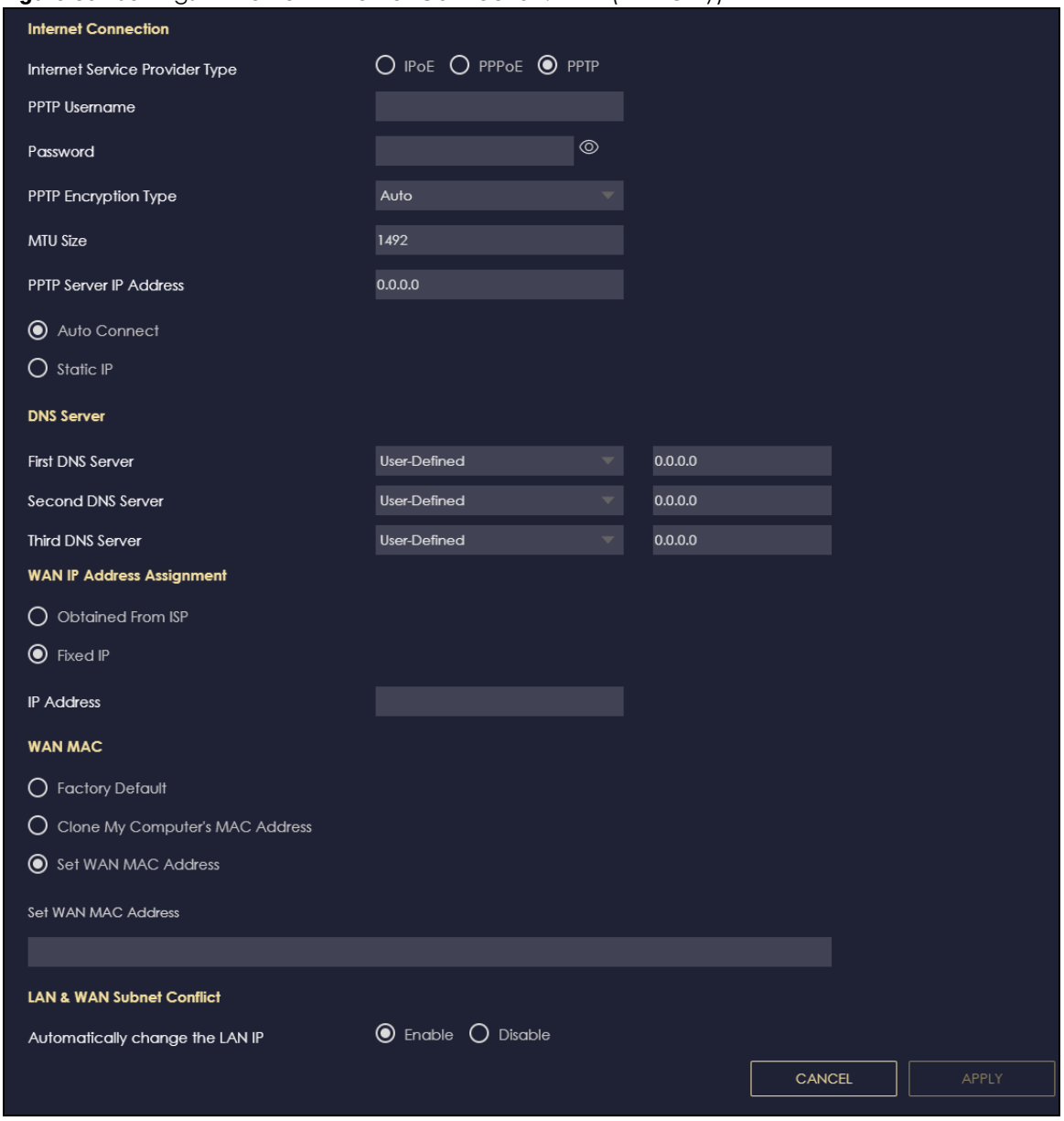
Table 26 Settings > Internet > Internet Connection: PPPoE

LABEL	DESCRIPTION
Automatically change the LAN IP	Select this option to have the NBG6818 change its LAN IP address to 10.0.0.1 or 192.168.123.1 accordingly when the NBG6818 gets a dynamic WAN IP address in the same subnet as the LAN IP address. See Section 9.3.1 on page 84 for more information. The NAT, DHCP server and firewall functions on the NBG6818 are still available in this mode.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

9.4.3 PPTP Encapsulation

This screen displays when you select **PPTP** encapsulation.

Figure 50 Settings > Internet > Internet Connection: PPTP (IPv4 Only)



The following table describes the labels in this screen.

Table 27 Settings > Internet > Internet Connection: PPTP

LABEL	DESCRIPTION
Internet Connection	
Internet Service Provider Type	Select **PPTP** if you want to connect the Internet via point to point tunneling protocol.
PPTP Username	Enter the user name given to you by your ISP.
Password	Enter the password associated with the user name above.
PPTP Encryption Type	Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: **Auto** - This ISP account adjusts the encryption type automatically. **None** - This ISP account does not use MPPE. **40** - This ISP account uses 40-bit MPPE. **128** - This ISP account uses 128-bit MMPE.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the NBG6818 divides it into smaller fragments.
PPTP Server IP Address	Enter the IP address of the PPTP server.
Auto Connect	Select this radio button if the PPTP server did not assign you a fixed IP address.
Static IP	Select this radio button if the PPTP server assigned an IP address for your Internet connection.
IP Address	Enter the IP address provided by the PPTP server.
IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway	Enter the gateway IP address in this field.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN IP Address Assignment	
Obtained from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Fixed IP	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **IP Address**.
WAN MAC Address Once the WAN MAC address is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.	
Factory Default	Select this option to have the WAN interface use the factory assigned default MAC address. By default, the NBG6818 uses the factory assigned MAC address to identify itself.
Clone My Computer's MAC Address	Select this option to have the WAN interface use a different MAC address by cloning the MAC address of another device or computer. Enter the IP address of the device or computer whose MAC you are cloning.
Set WAN MAC Address	Select this option to have the WAN interface use a manually specified MAC address. Enter the MAC address in the fields.
LAN & WAN Subnet Conflict	

Table 27 Settings > Internet > Internet Connection: PPTP (continued)

LABEL	DESCRIPTION
Automatically change the LAN IP	Select this option to have the NBG6818 change its LAN IP address to 10.0.0.1 or 192.168.123.1 accordingly when the NBG6818 gets a dynamic WAN IP address in the same subnet as the LAN IP address. See Section 9.3.1 on page 84 for more information. The NAT, DHCP server and firewall functions on the NBG6818 are still available in this mode.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

9.5 NAT & Port Forwarding Screen

Use Port Forwarding to forward incoming service requests from the Internet to the server(s) on your local network. Port forwarding is commonly used when you want to host online gaming, P2P file sharing, or other servers on your network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, DNS service is on port 53 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service, it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

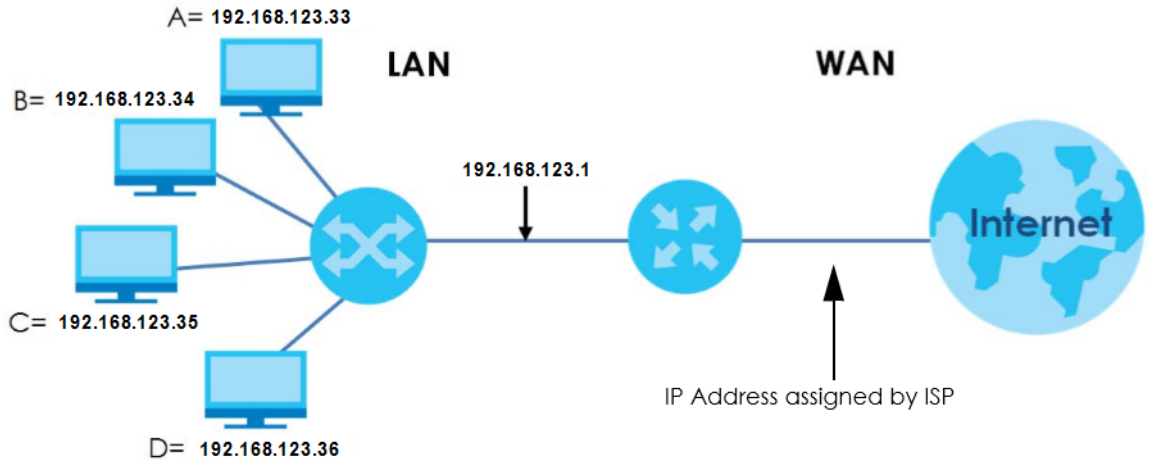
Note: TCP port 80, 443, 8008, 8099 and 8443 are reserved ports and cannot be used for NAT and firewall rules.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

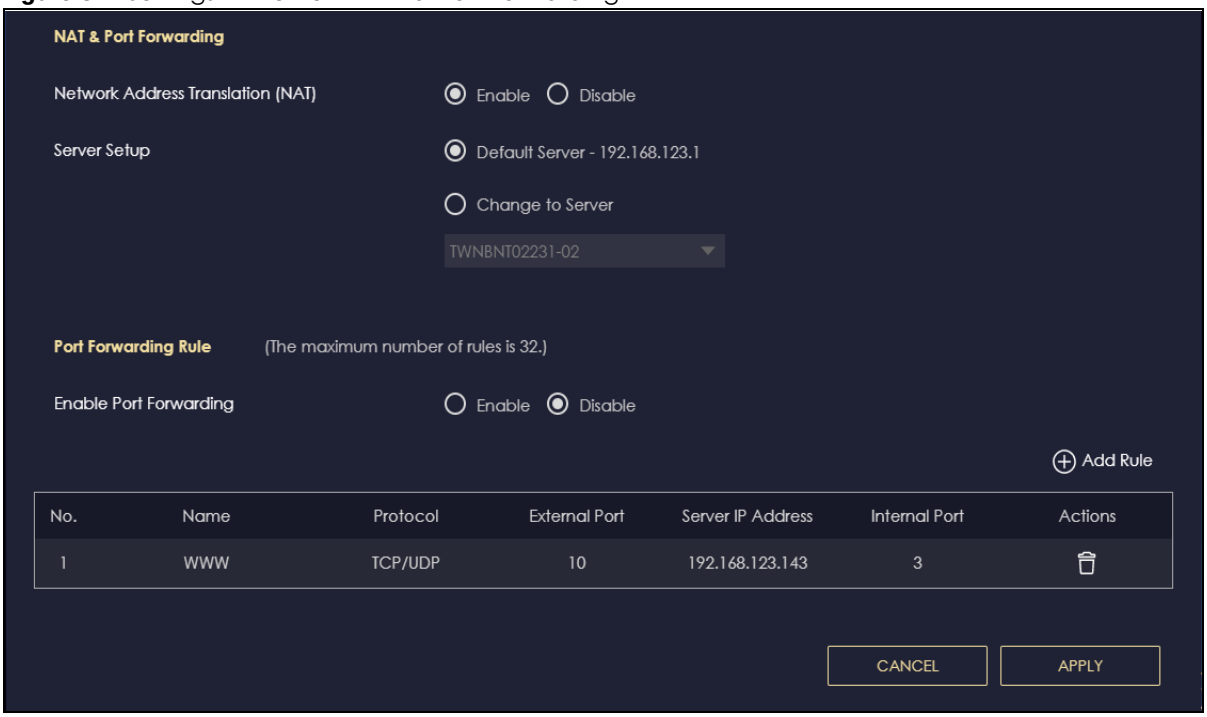
Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 60 to another (B in the example) and assign a default server IP address of 192.168.123.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 51 Multiple Servers Behind NAT Example



Use this screen to enable NAT, set a default server and view the summary table of your NBG6818's port forwarding settings. Click **Settings** > **Internet** > **NAT & Port Forwarding** to show the following screen.

Figure 52 Settings > Internet > NAT & Port Forwarding



The following table describes the labels in this screen.

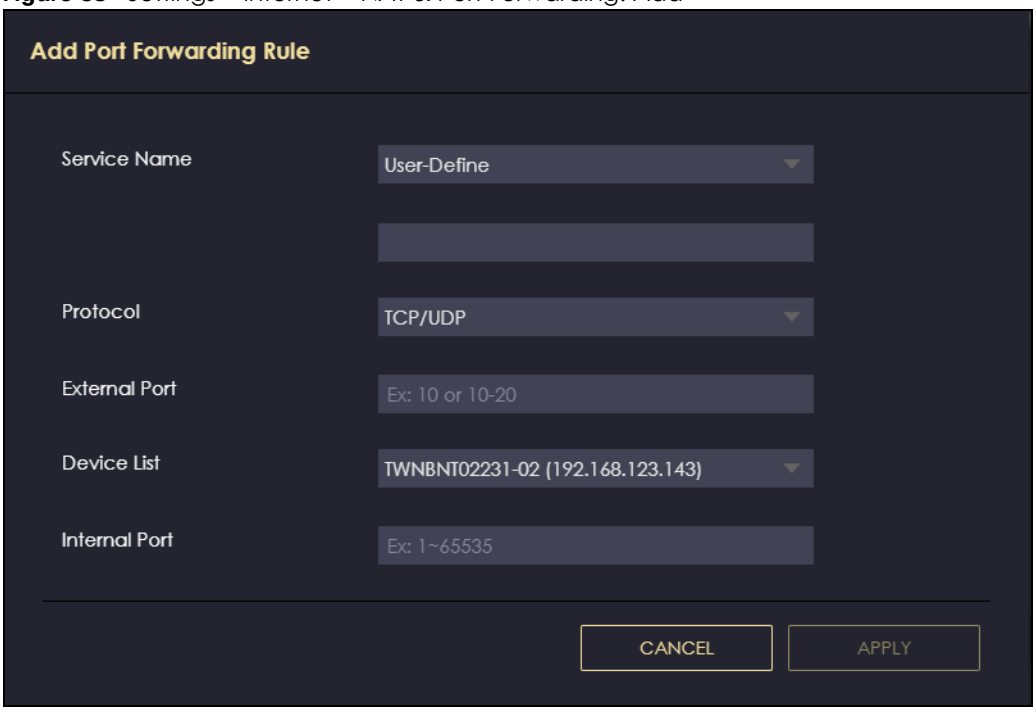
Table 28 Settings > Internet > NAT & Port Forwarding

LABEL	DESCRIPTION
NAT & Port Forwarding	
Network Address Translation (NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select **Enable** to activate NAT. Select **Disable** to turn it off.
Server Setup	
Default Server	You can decide whether you want to use the default server or specify a server manually. In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the port forwarding summary table below. Select this to use the default server.
Change To Server	Select this and manually enter the server's IP address.
Port Forwarding Rule	
Enable Port Forwarding	Select **Enable** to allow port forwarding. Otherwise, select **Disable**.
No.	This number uniquely identifies the port forwarding rule.
Name	This field displays a name to identify this rule.
Protocol	This is the transport layer protocol used for the service.
External Port	This is the port number used to connect to this service using the router's external IP address on the WAN.
Server IP Address	This field displays the internal IP address of the server.
Internal Port	This is the port number used to connect to this service using the server's internal IP address on the LAN.
Actions	Click the icons under **Actions** to delete or edit a port forwarding rule. Click  to delete the rule. Click  to edit the rule.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

9.5.1 Add Port Forwarding Rule Screen

Use this screen to configure your NBG6818's port forwarding settings to forward incoming service requests to the servers on your local network. Click **Settings** > **Internet** > **NAT & Port Forwarding** > **Add Rule** to show the following screen.

Figure 53 Settings > Internet > NAT & Port Forwarding: Add



The following table describes the labels in this screen.

Table 29 Settings > Internet > NAT & Port Forwarding: Add

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will be displayed in the port forwarding summary table. Otherwise, select **User-Define** to manually enter the port number/range and select the **Protocol**.
Protocol	Select the transport layer protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP_UDP**. If you have chosen a pre-defined service in the **Service Name** field, the protocol will be configured automatically.
External Port	This shows the port number used to connect to this service using the router's external IP address on the WAN. If you select **User-Define** in the **Service Name** field, enter the port number(s) manually.
Device List	Select the internal IP address of the virtual server.
Internal Port	This shows the port number used to connect to this service using the server's internal IP address on the LAN. If you select **User-Define** in the **Service Name** field, enter an internal port number manually or leave the field blank for port range forwarding.
APPLY	Click **APPLY** to save your changes.
CANCEL	Click **CANCEL** to exit this screen without saving.

9.6 Passthrough Screen

Use this screen to change your NBG6818's ALGs and VPN pass-through settings. Click **Settings** > **Internet** > **Passthrough** to show the following screen.

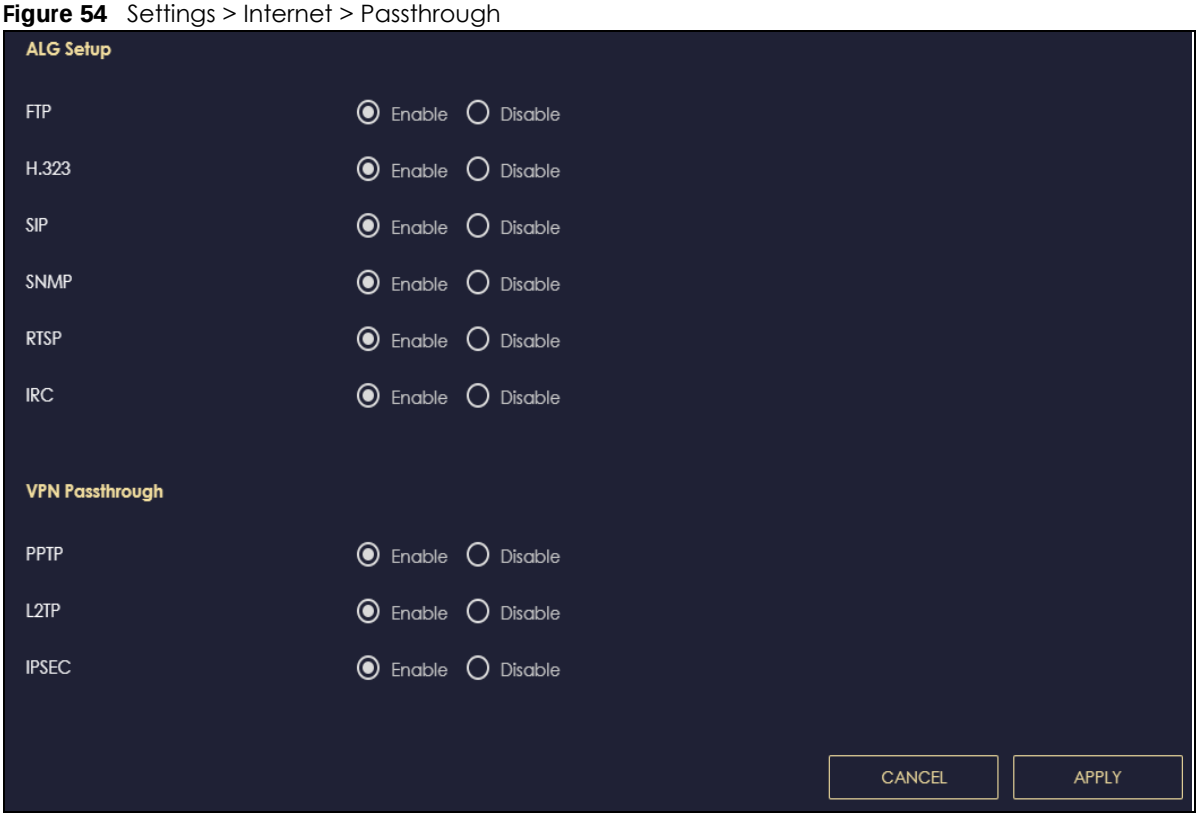
ALG Overview

Application Layer Gateway (ALG) allows the following applications to operate properly through the NBG6818's NAT.

- SIP - Session Initiation Protocol (SIP) - An application-layer protocol that can be used to create voice and multimedia sessions over Internet.
- H.323 - A teleconferencing protocol suite that provides audio, data and video conferencing.
- FTP - File Transfer Protocol - an Internet file transfer service.
- SNMP - Simple Network Management Protocol - An application-layer protocol that can be used to exchange management information between network devices.
- RTSP - Real Time Streaming Protocol - An application-layer protocol that can be used to stop, pause or play video and audio applications streaming on the Internet.
- IRC - Internet Relay Chat - An application-layer protocol that can control the relay chat applications and allow clients to have real-time communications with others on the Internet.

The ALG feature is only needed for traffic that goes through the NBG6818's NAT.

Figure 54 Settings > Internet > Passthrough



The following table describes the labels in this screen.

Table 30 Settings > Internet > Passthrough

LABEL	DESCRIPTION
ALG Setup	
FTP	Select **Enable** to allow TCP packets with a specified port destination to pass through.
H.323	Select **Enable** to allow peer-to-peer H.323 calls.
SIP	Select **Enable** to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
SNMP	Select **Enable** to allow a manager station to manage and monitor the NBG6818 through the network via SNMP.
RTSP	Select **Enable** to have the NBG6818 detect RTSP traffic and help build RTSP sessions through its NAT.
IRC	Select **Enable** to allow clients to have real-time communications with others on the Internet.
VPN Passthrough	
PPTP	Select **Enable** to allow VPN clients to make outbound PPTP connections. It is required in order to connect to a PPTP VPN account. If **PPTP** is disabled, then when a client sends a request to a VPN server, the server will reply to the NBG6818 and the NBG6818 will drop the request. When **PPTP** is enabled, the NBG6818 will forward the reply from the VPN server to the client that initiated the request, and the connection will establish successfully.
L2TP	Select **Enable** to allow VPN clients to make outbound L2TP connections. It is required in order to connect to a L2TP VPN account. If **L2TP** is disabled, then when a client sends a request to a VPN server, the server will reply to the NBG6818 and the NBG6818 will drop the request. When **L2TP** is enabled, the NBG6818 will forward the reply from the VPN server to the client that initiated the request, and the connection will establish successfully.
IPSEC	Select **Enable** to allow VPN clients to make outbound IPSec connections. It is required in order to connect to a IPSec VPN account. If **IPSEC** is disabled, then when a client sends a request to a VPN server, the server will reply to the NBG6818 and the NBG6818 will drop the request. When **IPSEC** is enabled, the NBG6818 will forward the reply from the VPN server to the client that initiated the request, and the connection will establish successfully.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

9.7 Port Trigger Screen

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

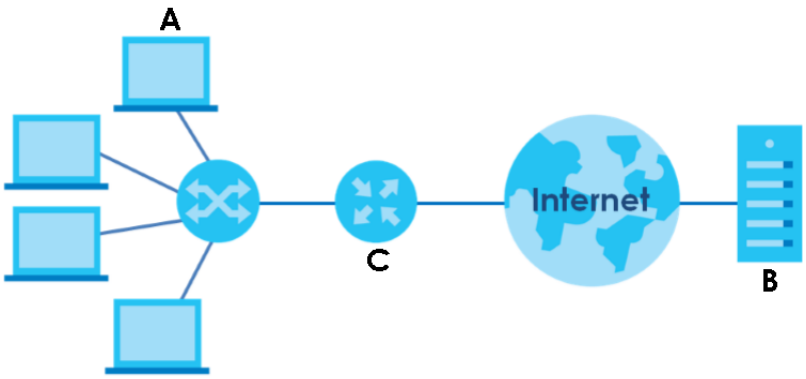
Trigger port forwarding addresses this problem. Trigger port forwarding allows computers on the LAN to dynamically take turns using the service. The NBG6818 records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the NBG6818's WAN port receives a response with a specific port number and protocol ("open" port), the NBG6818 forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

Note: TCP port 7547 is reserved for system use.

Note: The maximum number of trigger ports for a single rule or all rules is 999.

Note: The maximum number of open ports for a single rule or all rules is 999.

Figure 55 Port Trigger Process: Example



1 Jane (**A**) requests a file from the Real Audio server (**B** port 7070).

2 Port 7070 is a "trigger" port and causes the NBG6818 (**C**) to record Jane's computer IP address. The NBG6818 associates Jane's computer IP address with the "open" port range of 6970-7170.

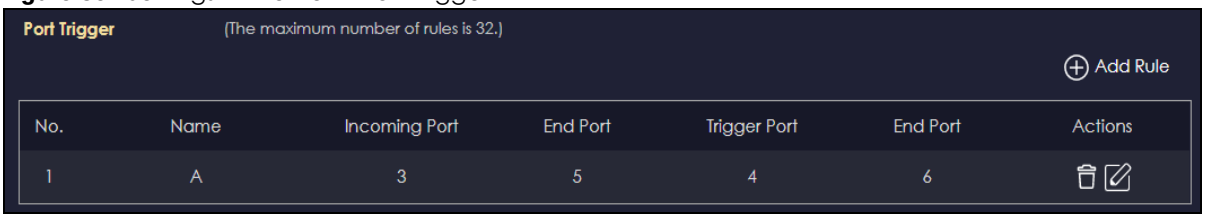
3 The Real Audio server responds using a port number ranging between 6970-7170.

4 TheNBG6818 forwards the traffic to Jane's computer IP address.Only Jane can connect to the Real Audio server until the connection is closed or times out. The NBG6818 times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Use this screen to view the summary table of your NBG6818's port trigger settings. Click **Expert Mode** > **WAN** > **NAT** > **Port Trigger** to show the following screen.

Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 56 Settings > Internet > Port Trigger



The following table describes the labels in this screen.

Table 31 Settings > Internet > Port Trigger

LABEL	DESCRIPTION
Port Trigger Rules (Max Limit: 32)	
No.	This is the rule index number.
Name	This field displays a name to identify this rule.

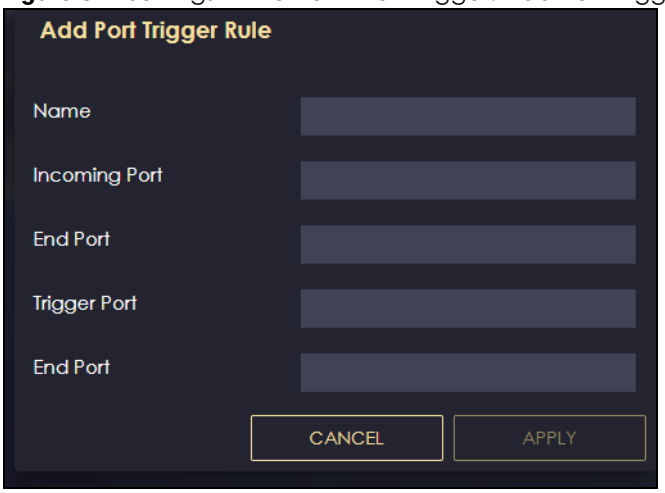
Table 31 Settings > Internet > Port Trigger (continued)

LABEL	DESCRIPTION
Incoming Port	This field displays a port number that a server on the WAN uses when it sends out a particular service.
End Port	This field displays a port number or the final port number in a range of port numbers.
Trigger Port	This field displays a port number that causes the NBG6818 to record the IP address of the LAN computer that sent then traffic to a server on the WAN.
End Port	This field displays a port number or the ending port number in a range of port numbers.
Actions	Click the icons under **Actions** to delete or edit an existing trigger port settings. Click to delete the rule. Click to edit the rule.

9.7.1 Add Port Trigger Rule Screen

Use this screen to configure your NBG6818's port trigger settings. Click **Add Rule** in the **Settings > Internet > Port Trigger** screen.

Figure 57 Settings > Internet > Port Trigger: Add Port Trigger Rule



The following table describes the labels in this screen.

Table 32 Settings > Internet > Port Trigger: Add Port Trigger Rule

LABEL	DESCRIPTION
Name	Enter a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming Port	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The NBG6818 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger Port	The trigger port is a port (or a range of ports) that causes (or triggers) the NBG6818 to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.

Table 32 Settings > Internet > Port Trigger: Add Port Trigger Rule (continued)

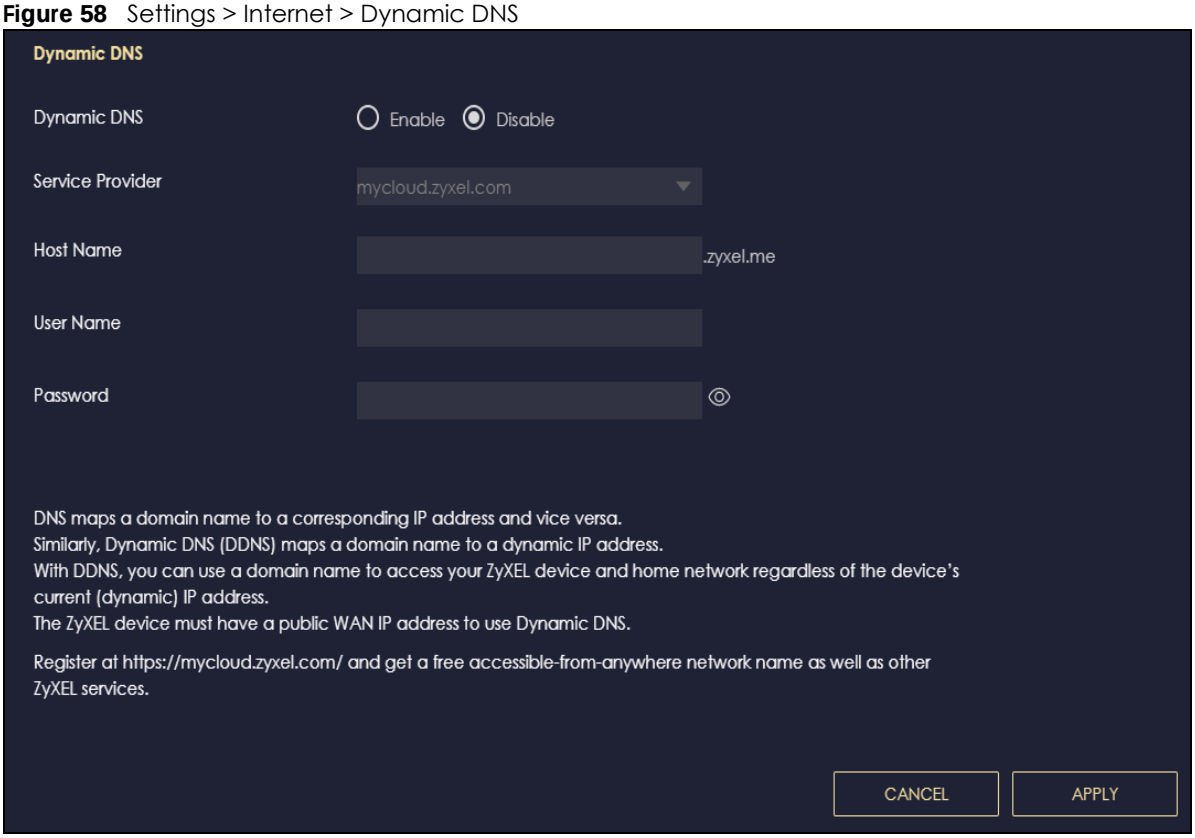
LABEL	DESCRIPTION
APPLY	Click **APPLY** to save your changes.
CANCEL	Click **CANCEL** to exit this screen without saving.

9.8 Dynamic DNS Screen

Use this screen to change your NBG6818's DDNS settings. Click **Settings** > **Internet** > **Dynamic DNS** to show the following screen.

Note: You can register at https://mycloud.zyxel.com/ to get a free accessible-from-anywhere DDNS account.

Figure 58 Settings > Internet > Dynamic DNS



The following table describes the labels in this screen.

Table 33 Settings > Internet > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select **Enable** to use dynamic DNS. Select **Disable** to turn this feature off.
Service Provider	Select the name of your Dynamic DNS service provider.

Table 33 Settings > Internet > Dynamic DNS (continued)

LABEL	DESCRIPTION
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

9.9 UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. A device can then leave a network smoothly and automatically when it is no longer in use.

See Section 9.9.1 on page 104 for more information on UPnP.

Use this screen to enable UPnP on your NBG6818. Click **Settings** > **Internet** > **UPnP** to display the following screen.

Figure 59 Settings > Internet > UPnP

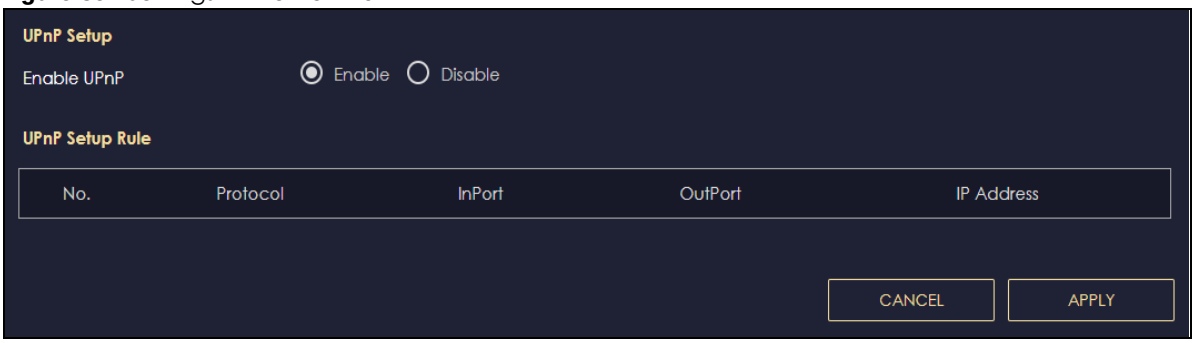


Table 34 Settings > Internet > UPnP

LABEL	DESCRIPTION
UPnP Setup	
Enable UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the NBG6818's IP address (although you must still enter the password to access the web configurator).
UPnP Setup Rule	
No.	This is the number of an individual UPnP entry.
Protocol	This is the transport layer protocol used for the service.
InPort	**InPort** is a port that a LAN computer uses when it requests a particular service. This port is only applicable to the local network. This field displays the port number of the UPnP entry.

Table 34 Settings > Internet > UPnP (continued)

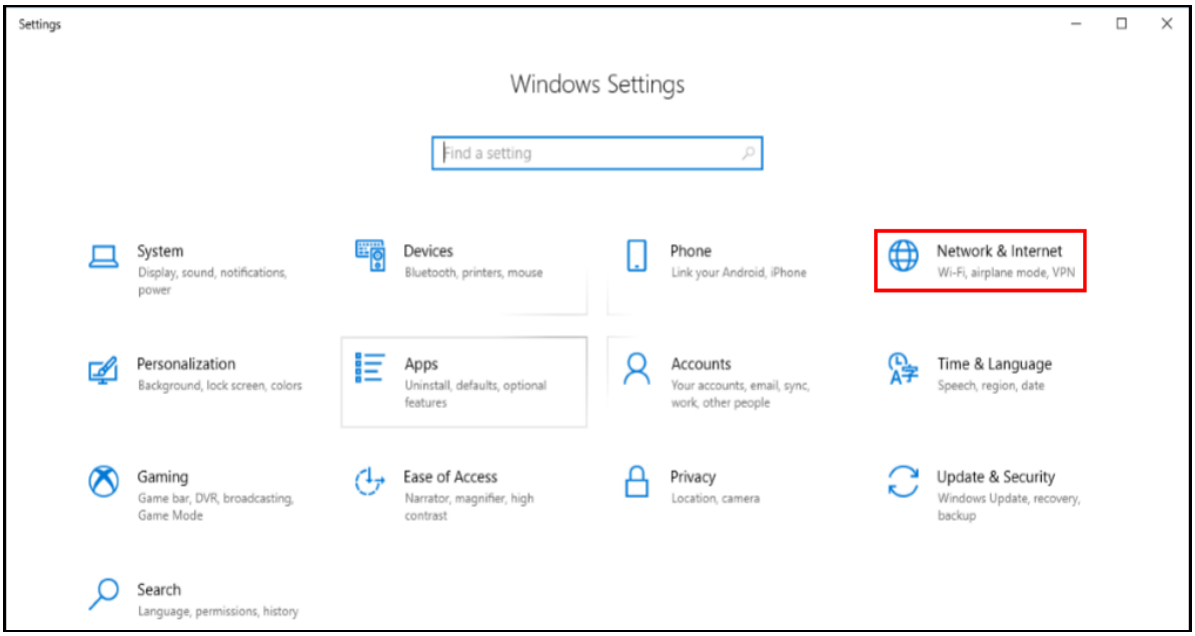
LABEL	DESCRIPTION
OutPort	**OutPort** is the well-known port that the WAN server uses to reply to the LAN computer that made the request using In Port. This field displays the port number of the UPnP entry.
IP Address	This field displays the IP address of this UPnP entry.
APPLY	Click **APPLY** to save your settings.
CANCEL	Click **CANCEL** to return to the previously saved settings.

9.9.1 Turning on UPnP in Windows 10 Example

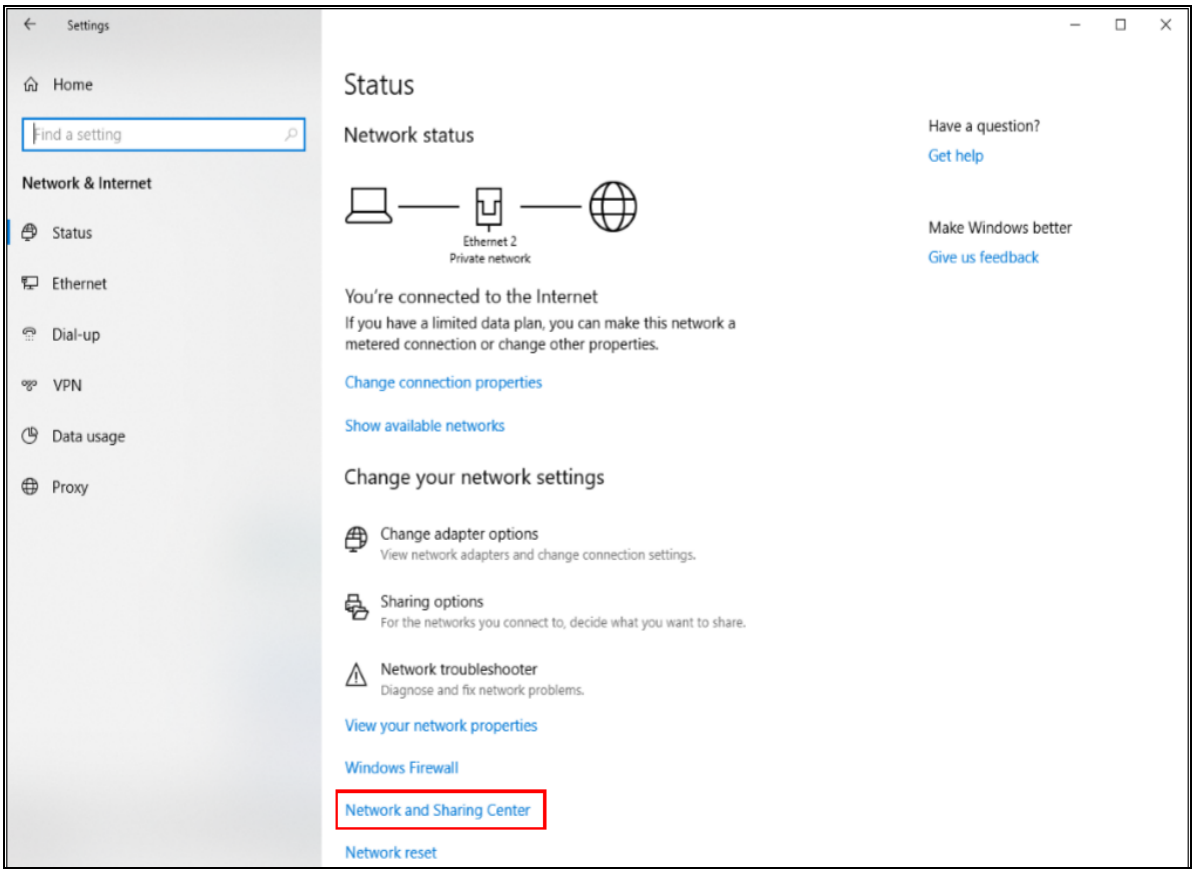
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the NBG6818 in **Settings** > **Internet** > **UPnP**.

Make sure the computer is connected to the LAN port of the NBG6818. Turn on your computer and the NBG6818.

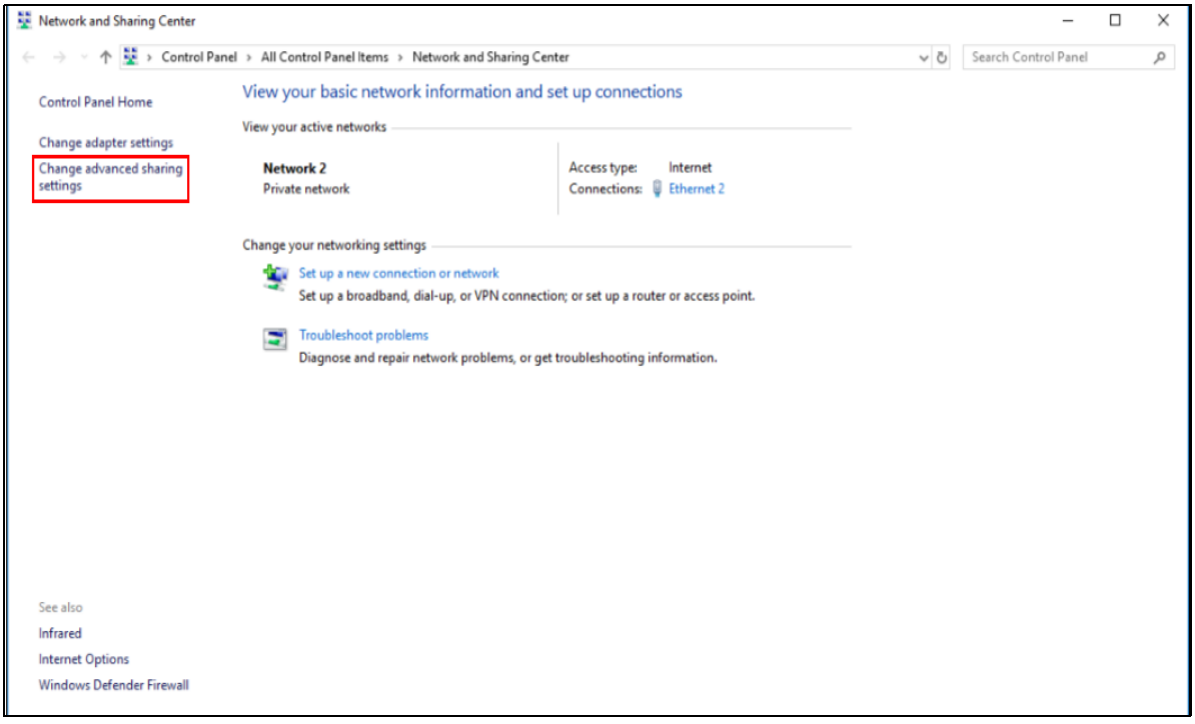
1 Click the start icon, **Settings** and then **Network & Internet**.



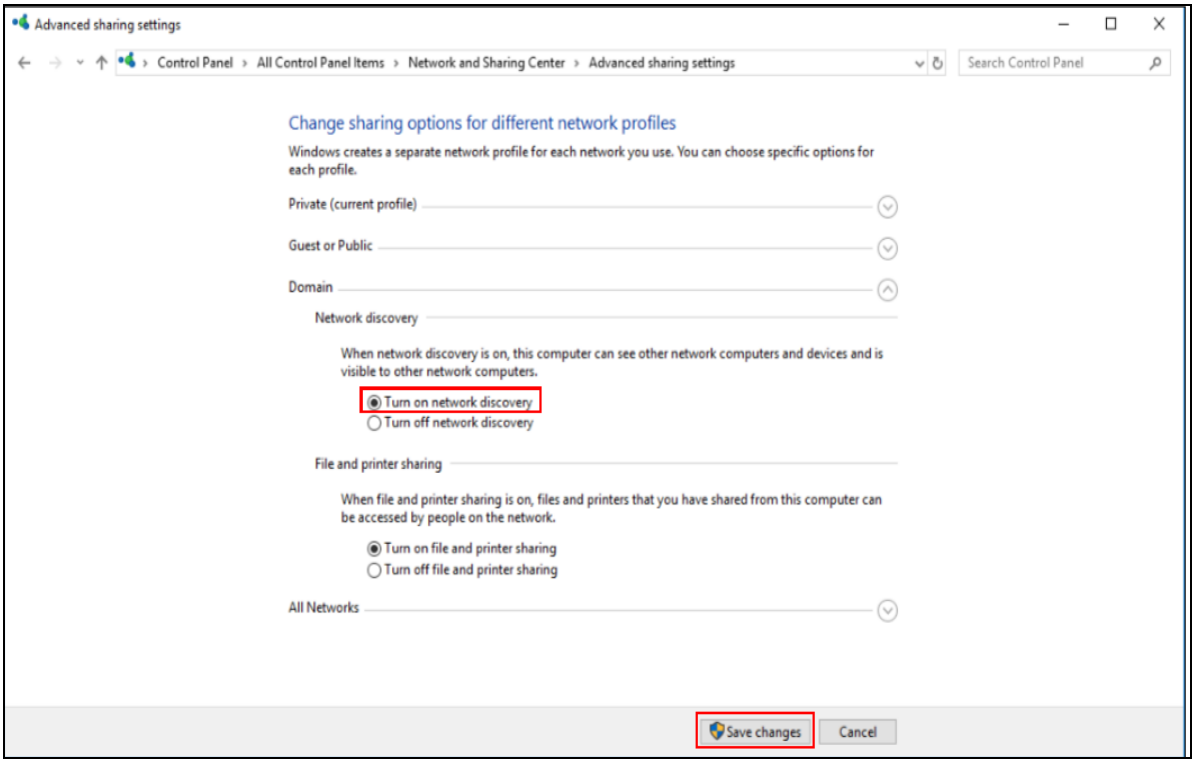
2 Click **Network and Sharing Center**.



3 Click **Change advanced sharing settings**.



4 Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.



CHAPTER 10
Wireless LAN

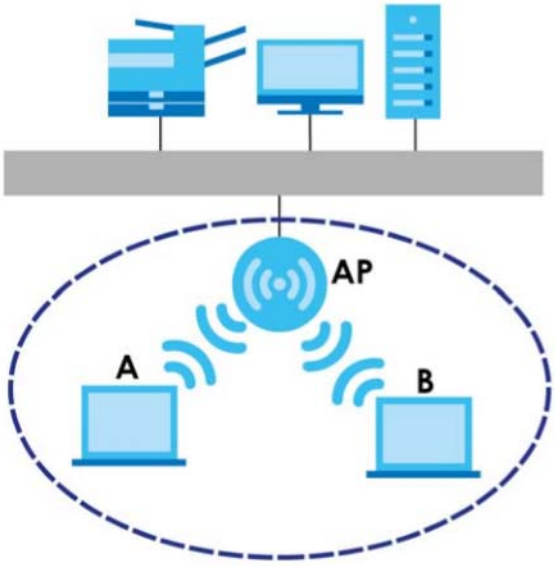
10.1 Overview

This chapter discusses how to configure the WiFi network settings in your NBG6818. The NBG6818 can service both 2.4G and 5G networks at the same time. You can have different WiFi setup and settings for 2.4G and 5G WiFi. Click **Settings > WiFi** to configure **wireless LAN 2.4G** or **wireless LAN 5G**.

See the appendices for more detailed information about WiFi networks.

The following figure provides an example of a WiFi network.

Figure 60 Example of a WiFi Network



The WiFi network in the figure is encircled in blue. In this WiFi network, devices **A** and **B** are called WiFi clients. The WiFi clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your NBG6818 is the AP.

10.1.1 What You Can Do

- Use the **Main WiFi** screen to enable or disable the 2.4 GHz or 5 GHz WiFi, set up WiFi security between the NBG6818 and the WiFi clients, and make other basic configuration changes (Section 10.2 on page 111).
- Use the **Guest WiFi** screen to set up multiple WiFi networks on your NBG6818 (Section 10.3 on page 112).
- Use the **MAC Filter** screen to allow or deny WiFi stations from connecting to the NBG6818 based on their MAC address (Section 10.4 on page 113).

- Use the **WPS** screen to quickly set up a WiFi network with strong security without having to configure security settings manually (Section 10.5 on page 114).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 10.6 on page 116).

10.1.2 What You Should Know

Every WiFi network must follow these basic guidelines.

- Every WiFi client in the same WiFi network must use the same Service Set Identifier (SSID).

  The SSID is the name of the WiFi network.
- If two WiFi networks overlap, they should use different channels.

  Like radio stations or television channels, each WiFi network uses a specific channel, or frequency, to send and receive information.
- Every WiFi client in the same WiFi network must use security compatible with the AP.

  Security stops unauthorized devices from using the WiFi network. It also protects information that is sent through the WiFi network.

WiFi Security Overview

The following sections introduce different types of WiFi security you can set up in the WiFi network.

SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the WiFi network.

MAC Address Filter

Every WiFi client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each WiFi client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which WiFi clients are allowed or not allowed to use the WiFi network. If a WiFi client is allowed to use the WiFi network, it still has to have the correct settings (SSID, channel, and security). If a WiFi client is not allowed to use the WiFi network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the WiFi network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized WiFi client. Then, they can use that MAC address to use the WiFi network.

1. Some WiFi devices, such as scanners, can detect WiFi networks but cannot use WiFi networks. These kinds of WiFi devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

User Authentication

You can make every user log in to the WiFi network before they can use it. This is called user authentication. However, every WiFi client in the WiFi network has to support IEEE 802.1x to do this.

For WiFi networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the WiFi network, even if they cannot use the WiFi network. Furthermore, there are ways for unauthorized WiFi users to get a valid user name and password. Then, they can use that user name and password to use the WiFi network.

Local user databases also have an additional limitation that is explained in the next section.

Encryption

WiFi networks can use encryption to protect the information that is sent in the WiFi network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The WPA-PSK (WiFi Protected Access-Pre-Shared Key) security mode provides both improved data encryption and user authentication over WEP. Using a pre-shared key, both the NBG6818 and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be. The WPA3-SAE (Simultaneous Authentication of Equals handshake) is the newer security mode that protects against dictionary attacks by implementing a new key exchange protocol.

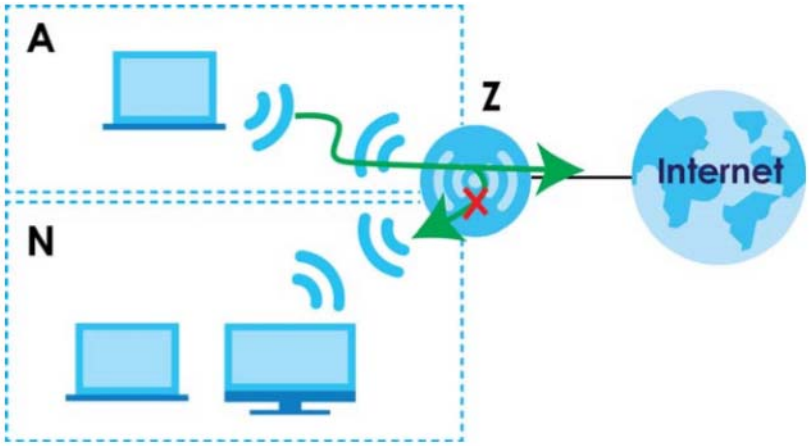
Guest WiFi

Guest WiFi allows you to set up a WiFi network where users can access to Internet via the NBG6818 (**Z**), but not other networks connected to it. In the following figure, a guest user can access the Internet from the guest WiFi network **A** via **Z** but not the home or company network **N**.

Note: The home or company network **N** and Guest WiFi network are independent networks.

Note: Only standard (router) mode supports guest WiFi.

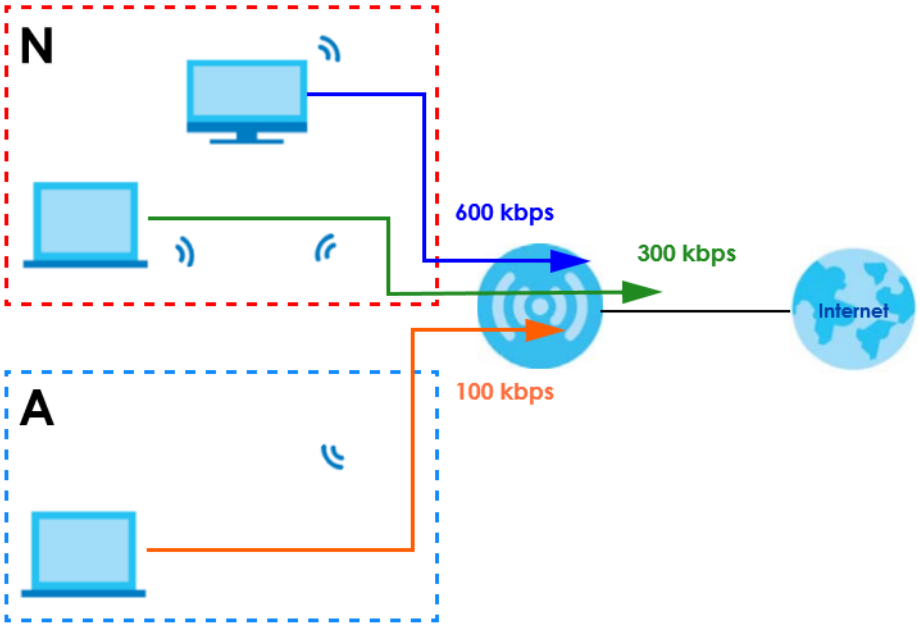
Figure 61 Guest WiFi LAN Network



Guest WiFi Bandwidth

The Guest WiFi Bandwidth function allows you to restrict the maximum bandwidth for the guest WiFi network. Additionally, you can also define bandwidth for your home or office network. An example is shown in the next figure to define maximum bandwidth for your networks (**A** is Guest WiFi and **N** is a home or company network.)

Figure 62 Example: Bandwidth for Different Networks



WPS

WiFi Protected Setup (WPS) is an industry standard specification defined by the WiFi Alliance. WPS allows you to set up a WiFi network with strong security without having to configure security settings manually. Depending on the client devices in your network, you can either press a button (on the client device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the client devices. They then connect and set up a secure network by themselves. See how to set up a secure WiFi network using WPS in Section 4.2 on page 35.

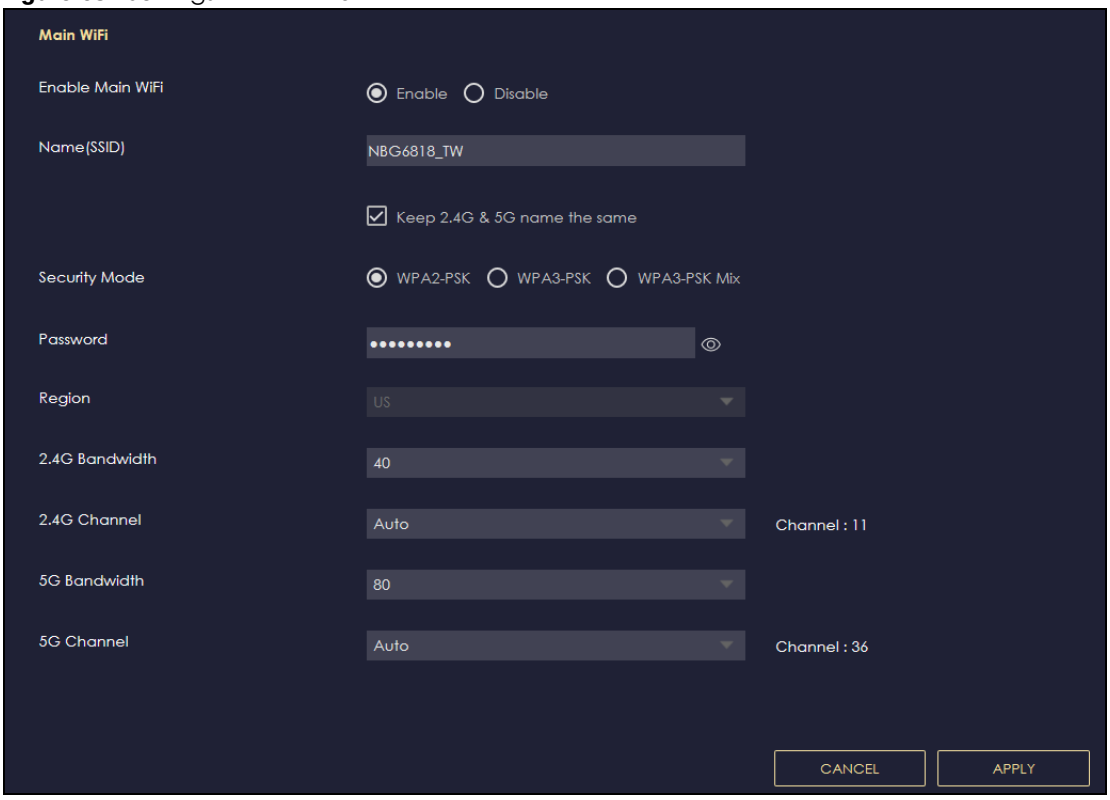
10.2 Main WiFi Screen

Use this screen to configure the SSID and WiFi security of the NBG6818's default wireless LAN.

Note: If you are configuring the NBG6818 from a computer connected to the wireless LAN and you change the NBG6818's SSID, channel or security settings, you will lose your WiFi connection when you press **APPLY** to confirm. You must then change the WiFi settings of your computer to match the NBG6818's new settings.

Click **Settings** > **WiFi** > **Main WiFi** to show the following screen.

Figure 63 Settings > WiFi > Main WiFi



The following table describes the labels in this screen.

Table 35 Settings > WiFi > Main WiFi

LABEL	DESCRIPTION
Main WiFi	
Enable Main WiFi	Select **Enable** to activate the 2.4G and/or 5G WiFi. Select **Disable** to turn it off.
2.4G/5G Name (SSID)	The Service Set Identity (SSID) identifies the wireless LAN with which a WiFi client is associated. Enter a name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN. Click the **Keep 2.4G & 5G name the same** check box to use the same SSID for 2.4G and 5G WiFi network.
Security Mode	Select the security mode you want to apply to the NBG6818.

Table 35 Settings > WiFi > Main WiFi

LABEL	DESCRIPTION
Password	The password has two uses: • Manual: Manually enter the same password on the NBG6818 and the client. Enter 8-63 ASCII characters or exactly 64 hexadecimal ('0-9', 'a-f') characters. • WPS: When using WPS, the NBG6818 sends this password to the client. Click the eye icon to show or hide the password of your WiFi network. When the eye icon is slashed, you'll see the password in plain text. Otherwise, it is hidden.
Region	The country is set to US by default.
2.4G/5G Bandwidth	Select a bandwidth from the drop-down list box. The options vary depending on the frequency band you want to apply to the NBG6818.
2.4G/5G Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band you want to apply to the NBG6818.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to reload the previous configuration for this screen.

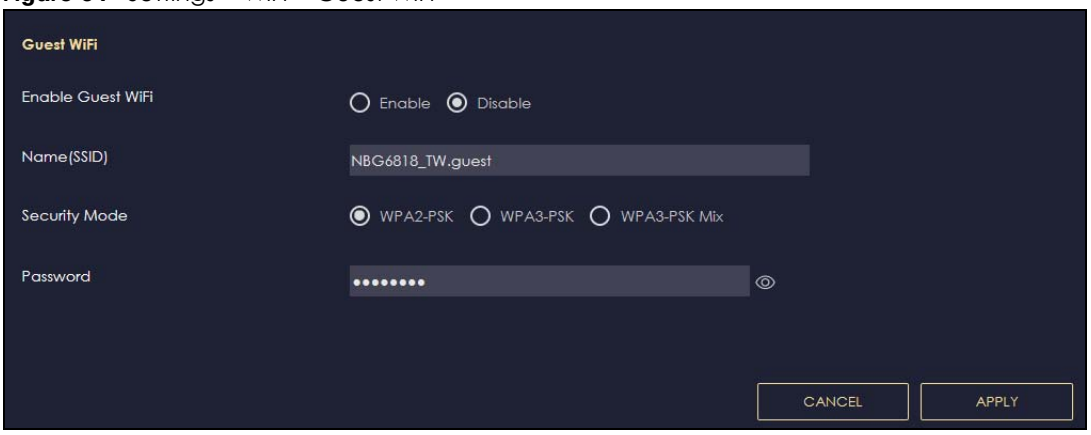
10.3 Guest WiFi Screen

This screen allows you to enable and configure guest WiFi network settings on the NBG6818.

Click **Settings** > **WiFi** > **Guest WiFi** to show the following screen.

Note: This is not available if you are using bridge mode.

Figure 64 Settings > WiFi > Guest WiFi



The following table describes the labels in this screen.

Table 36 Settings > WiFi > Guest WiFi

LABEL	DESCRIPTION
Enable Guest WiFi	Select **Enable** to activate the guest WiFi. Select **Disable** to turn it off.
Name (SSID)	An SSID profile is the set of parameters relating to one of the NBG6818's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a WiFi device is associated. This field displays the name of the WiFi profile on the network. When a WiFi client scans for an AP to associate with, this is the name that is broadcast and seen in the WiFi client utility.

Table 36 Settings > WiFi > Guest WiFi (continued)

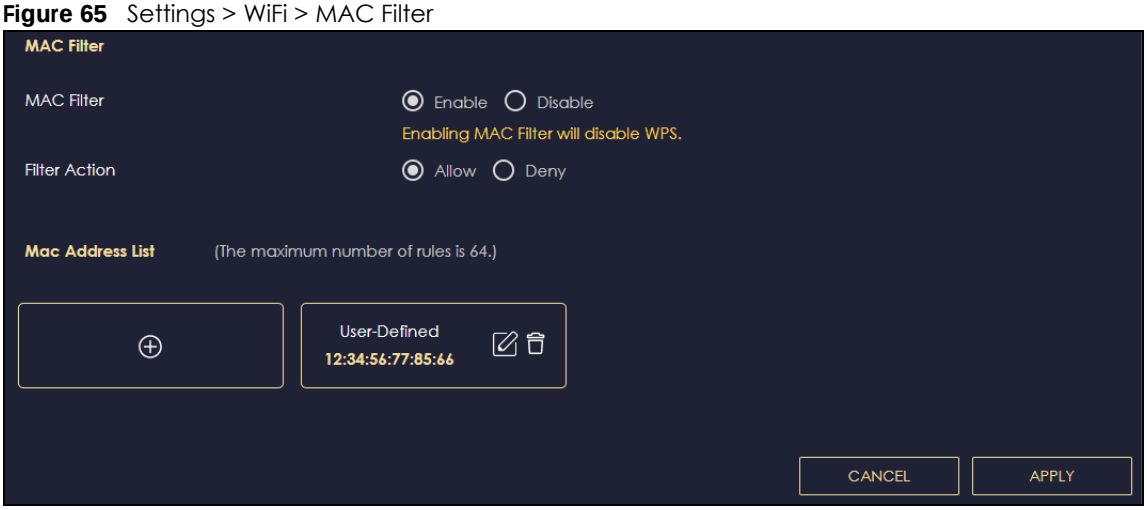
LABEL	DESCRIPTION
Password	The password has two uses. • Manual: Manually enter the same password on the NBG6818 and the client. Enter 8-63 ASCII characters or exactly 64 hexadecimal ('0-9', 'a-f') characters. • WPS: When using WPS, the NBG6818 sends this password to the client. Click the **Eye** icon to show or hide the password of your WiFi network. When the **Eye** icon is slashed, you'll see the password in plain text. Otherwise, it is hidden.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to reload the previous configuration for this screen.

10.4 MAC Filter Screen

The MAC filter screen allows you to give exclusive access to devices (**Allow**) or exclude devices from accessing the NBG6818 (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

Use this screen to change your NBG6818's MAC filter settings. Click **Settings** > **WiFi** > **MAC Filter** to show following screen.

Figure 65 Settings > WiFi > MAC Filter



The following table describes the labels in this screen.

Table 37 Settings > WiFi > MAC Filter

LABEL	DESCRIPTION
MAC Filter	Select to turn on (**Enable**) or off (**Disable**) MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Filter Summary** table. Select **Allow** to permit access to the NBG6818. MAC addresses not listed will be denied access to the NBG6818. Select **Deny** to block access to the NBG6818. MAC addresses not listed will be allowed to access the NBG6818.

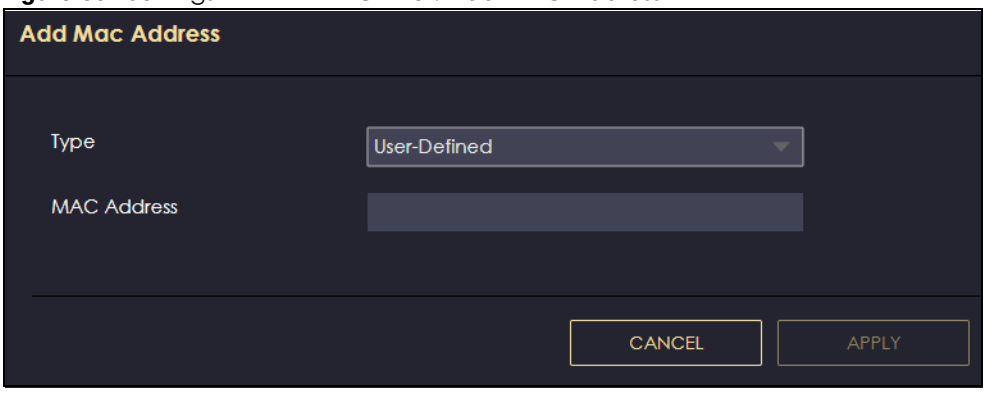
Table 37 Settings > WiFi > MAC Filter (continued)

LABEL	DESCRIPTION
MAC Address List (Max Limit : 64)	
	This field displays the MAC address of the WiFi station you want to filter. Click to configure the MAC address. Click to delete the MAC address.
Add	Click to add a rule in the **MAC Address List**.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to reload the previous configuration for this screen.

10.4.1 Add MAC Address Screen

Use this screen to configure the MAC address you want to add to the MAC address list. Click the icon in the **Settings** > **WiFi** > **MAC Filter** screen. The following screen appears.

Figure 66 Settings > WiFi > MAC Filter: Add MAC Address



The following table describes the labels in this screen.

Table 38 Settings > WiFi > MAC Filter: Add MAC Address

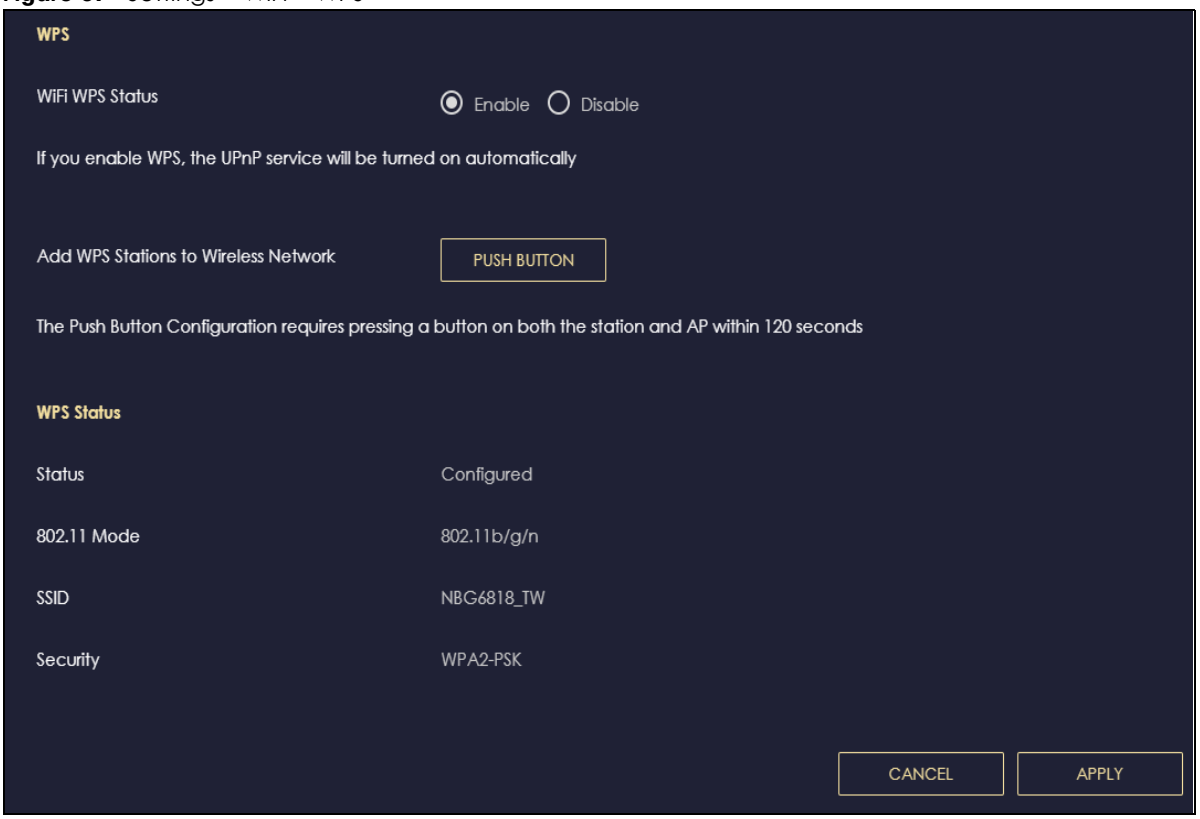
LABEL	DESCRIPTION
Type	This field displays the MAC address of the WiFi station. If you select **User-Defined**, enter the MAC address(es) manually.
MAC Address	Enter a MAC address manually in this field if you select **User-Defined** in the **Type** field.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to exit this screen without saving.

10.5 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN and check the current WPS status. Click **Settings** > **WiFi** > **WPS** to show the following screen.

Note: With WPS, WiFi clients can only connect to the WiFi network using the first SSID on the NBG6818.

Figure 67 Settings > WiFi > WPS



The following table describes the labels in this screen.

Table 39 Settings > WiFi > WPS

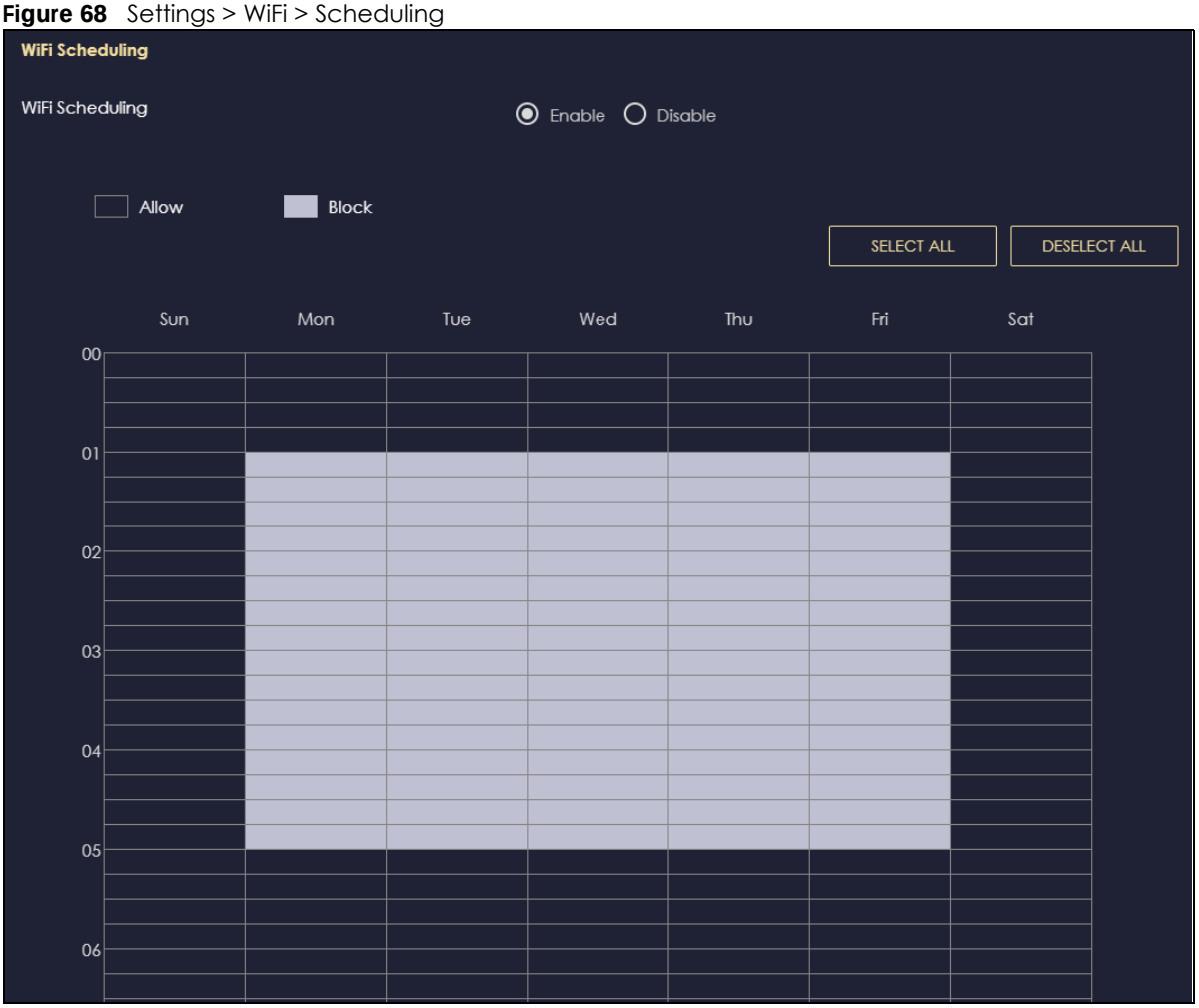
LABEL	DESCRIPTION
WPS	
WiFi WPS Status	Select **Enable** to turn on the WPS feature. Otherwise, select **Disable**.
Push Button	Use this button when you use the PBC (Push Button Configuration) method. Click this to start WPS-aware WiFi station scanning and WiFi security information synchronization.
WPS Status	
Status	This displays **Configured** when a WiFi station has connected to the NBG6818 using WPS and WiFi setup or security settings have been changed from default. The current WiFi setup and security settings also appear in this screen. This displays **Unconfigured** if WPS is disabled and there are no WiFi setup or security changes on the NBG6818 or if you click **Release Configuration** to restore WiFi setup and security settings to default.
802.11 Mode	This is the 802.11 mode used. Only compliant WiFi devices can associate with the NBG6818.
SSID	This is the name of the WiFi network (the NBG6818's first SSID) that WPS clients connect to.
Security	This is the type of WiFi security employed by the network.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to reload the previous configuration for this screen.

10.6 Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. The y-axis shows the time period in days. The x-axis shows the time period in hours. Click on the boxes to select the time period.

Click **Settings > WiFi > Scheduling** to show the following screen.

Figure 68 Settings > WiFi > Scheduling



The following table describes the labels in this screen.

Table 40 Settings > WiFi > Scheduling

LABEL	DESCRIPTION
WiFi Scheduling	Select **Enable** to activate the WiFi scheduling feature. Select **Disable** to turn it off.
SELECT ALL	Click **SELECT ALL** or click gray blocks to specify days and times to turn the WiFi on or off. If you click **SELECT ALL** you can not select any specific days and times.
DESELECT ALL	Click **DESELECT ALL** to remove all the WiFi scheduling.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to reload the previous configuration for this screen.

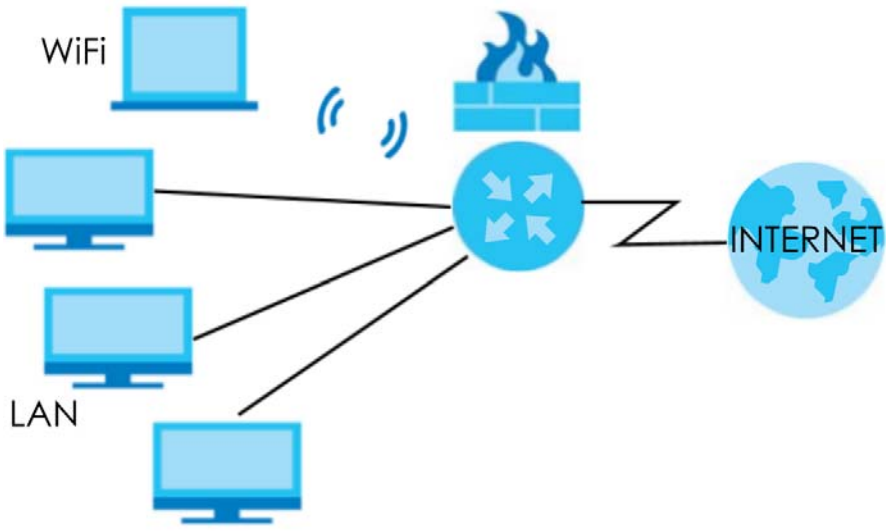
CHAPTER 11
LAN

11.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are connected. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building.

Figure 69 LAN Example



The LAN screens can help you configure a manage IP addresses and partition your physical network into logical networks.

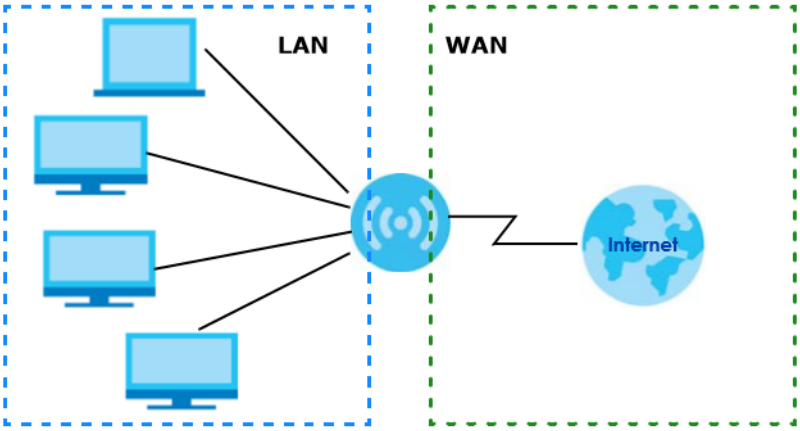
11.2 What You Can Do

- Use the **LAN IP** screen to configure the IP addresses for your NBG6818 on the LAN (Section 11.4 on page 118).
- Use the **IPv6 LAN** screen to configure the IPv6 address for your NBG6818 on the LAN (Section 11.5 on page 124).

11.3 What You Need To Know

The actual physical connection determines whether the NBG6818 ports are LAN or WAN ports. There are two separate IP networks: one inside the LAN network and the other outside the WAN network as shown in the following figure.

Figure 70 LAN and WAN IP Addresses



The LAN parameters of the NBG6818 are preset in the factory with the following values:

- IPv4 address of 192.168.123.1 with subnet mask of 255.255.255.0 (24 bits).
- DHCP server enabled with 128 client IPv4 addresses starting from 192.168.123.33.

These parameters should work for the majority of installations.

11.4 LAN IP Screen

Use this screen to change the IP address for your NBG6818 in Standard Mode. Click **Settings > LAN > LAN IP** to show the following screen.

Figure 71 Settings > LAN > LAN IP (Standard Mode)

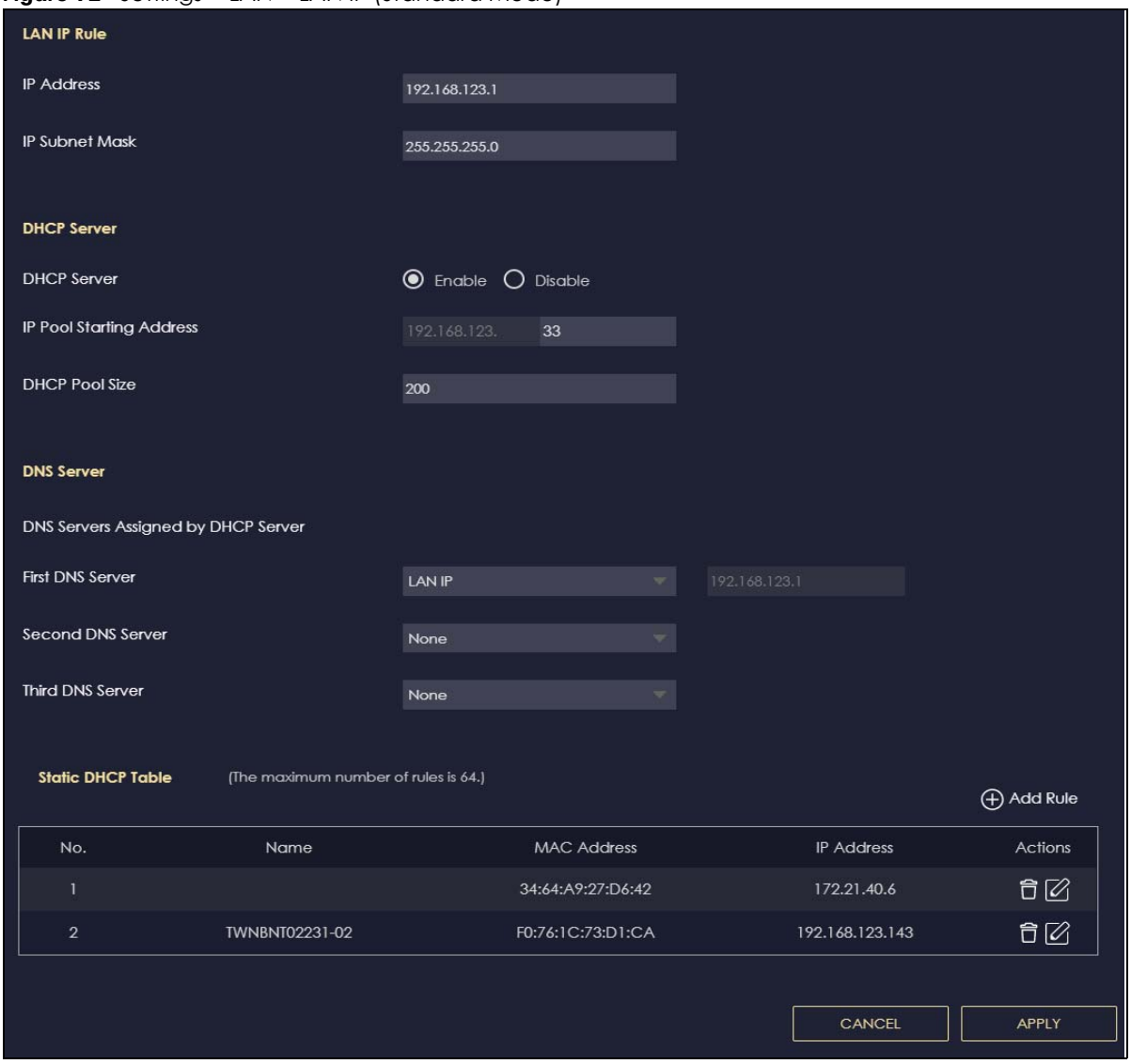
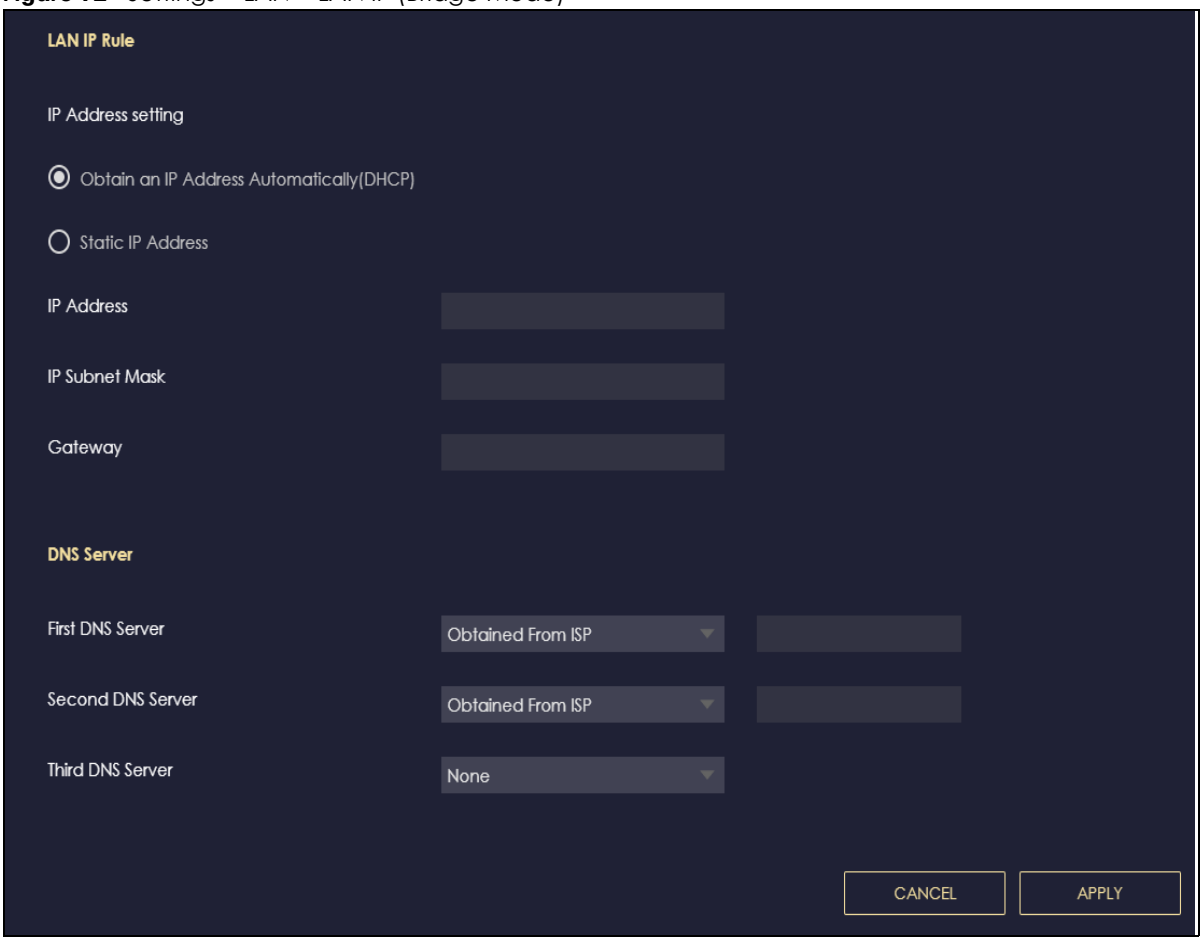


Figure 72 Settings > LAN > LAN IP (Bridge Mode)



The following table describes the labels in this screen.

Table 41 Settings > LAN > LAN IP

LABEL	DESCRIPTION
LAN IP Rule	
IP Address	Enter the IP address of your NBG6818 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG6818 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG6818.
DHCP Server Note: This is not available if you are using bridge mode.	
DHCP Server	Select **Enable** to activate DHCP for LAN. Select **Disable** to stop the NBG6818 from acting as a DHCP server. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Enable the DHCP server unless your ISP instructs you to do otherwise. When configured as a server, the NBG6818 provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.

Table 41 Settings > LAN > LAN IP (continued)

LABEL	DESCRIPTION
DHCP Pool Size	This field specifies the size, or count of the IP address pool for LAN.
DNS Server DNS Servers Assigned by DHCP Server	
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the NBG6818's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **LAN IP** and the field to the right displays the (read-only) default gateway IP address of your computer. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Static DHCP Table Note: This is not available if you are using bridge mode.	
No.	This is the index number of the static IP table entry (row).
Name	This field displays a name to identify this rule.
MAC Address	This field displays the MAC address of a computer on your LAN, or the MAC address you manually configured.
IP Address	This field displays the LAN IP address of a computer on your LAN, or the LAN address you manually configured.
Actions	Click the icons under **Actions** to delete or edit an existing static IP. Click  to delete an existing static IP. Click  to edit an existing static IP.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

11.4.1 Static DHCP Table-Add/Edit Rule Screen

Use this screen to configure the static DHCP. Click **Settings** > **LAN** > **LAN IP** > **Add Rule** or **Settings** > **LAN** > > **LAN IP** > **Edit** to show the following screens.

Note: This is not available if you are using bridge mode.

Figure 73 Settings > LAN > LAN IP: Add Rule

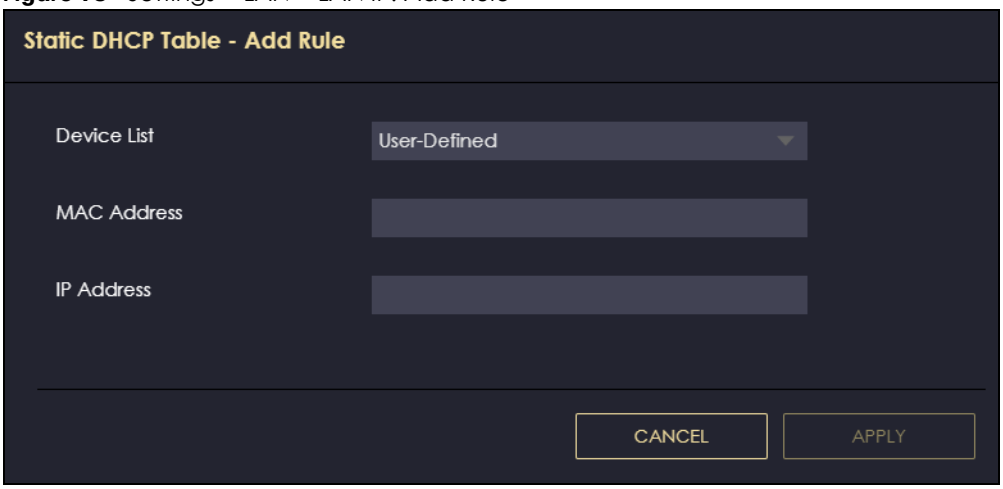
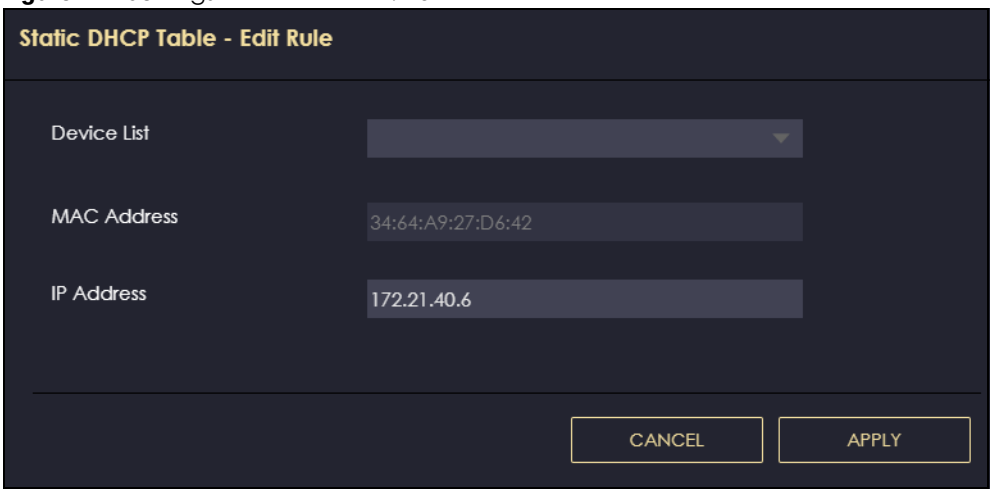


Figure 74 Settings > LAN > LAN IP: Edit



The following table describes the labels in these screens.

Table 42 Settings > LAN > LAN IP: Add Rule/Edit

LABEL	DESCRIPTION
Device LIst	This field lists the system name of the LAN user device which is connected to the NBG6818 and assigned an IP address. Select a LAN user device from the list to automatically detect the MAC address of a computer on your LAN. Otherwise, select **User-Defined** to enter the MAC address of a computer on your LAN in the **MAC Address** field.
MAC Address	This field displays the MAC address of a computer on your LAN. If you select **User-Defined** in the **Device List** field, enter the MAC address(es) manually.
IP Address	This field displays the IP address of a computer on your LAN. If you select **User-Defined** in the **Device List** field, enter the IP address(es) manually.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to exit this screen without saving.

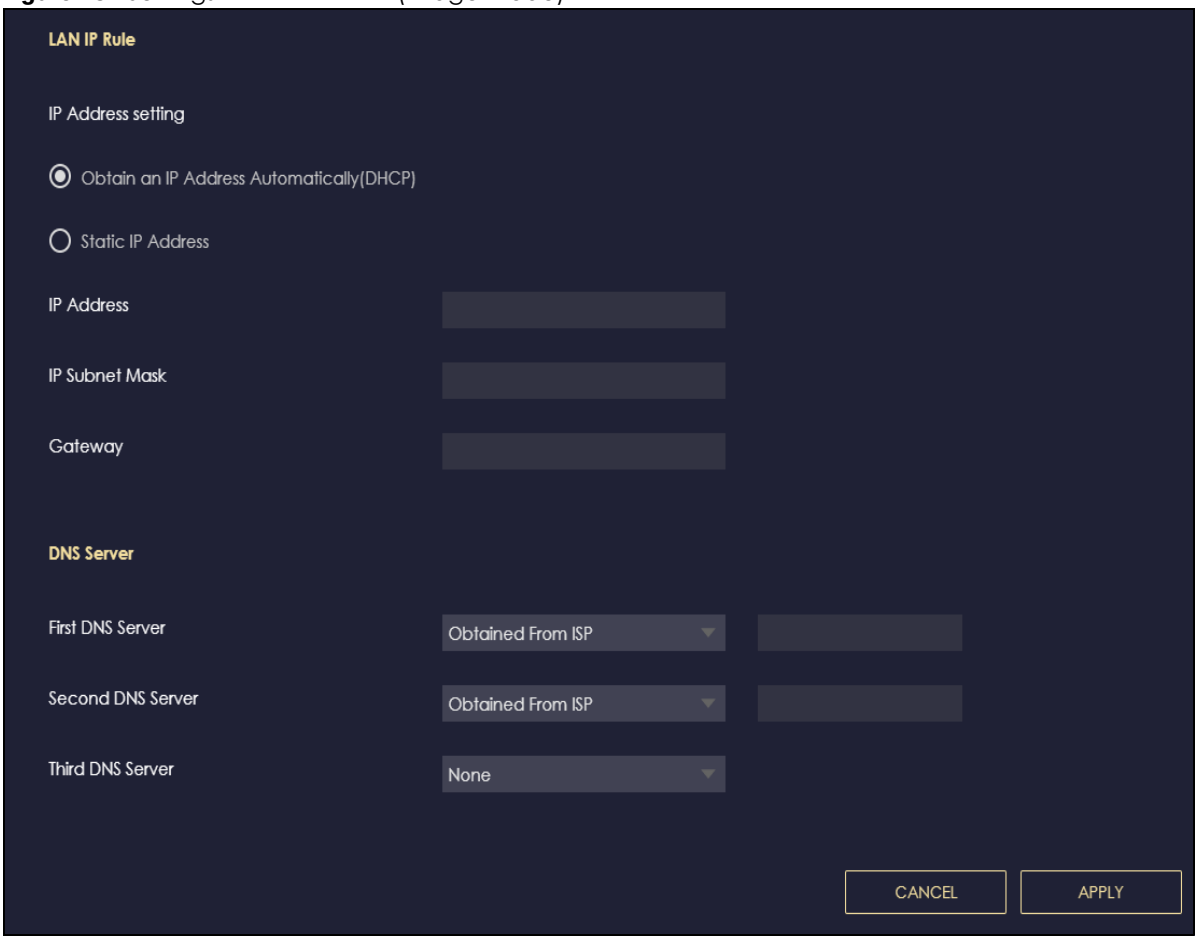
11.4.2 Configure LAN Screen in Bridge Mode

Use this section to configure your LAN settings while in **Bridge Mode**.

Click **Settings > LAN > LAN IP** to show the following screen.

Note: If you change the IP address of the NBG6818 in the screen below, you will need to log into the NBG6818 again using the new IP address.

Figure 75 Settings > LAN > LAN IP (Bridge Mode)



The table below describes the labels in the screen.

Table 43 Settings > LAN > LAN IP (Bridge Mode)

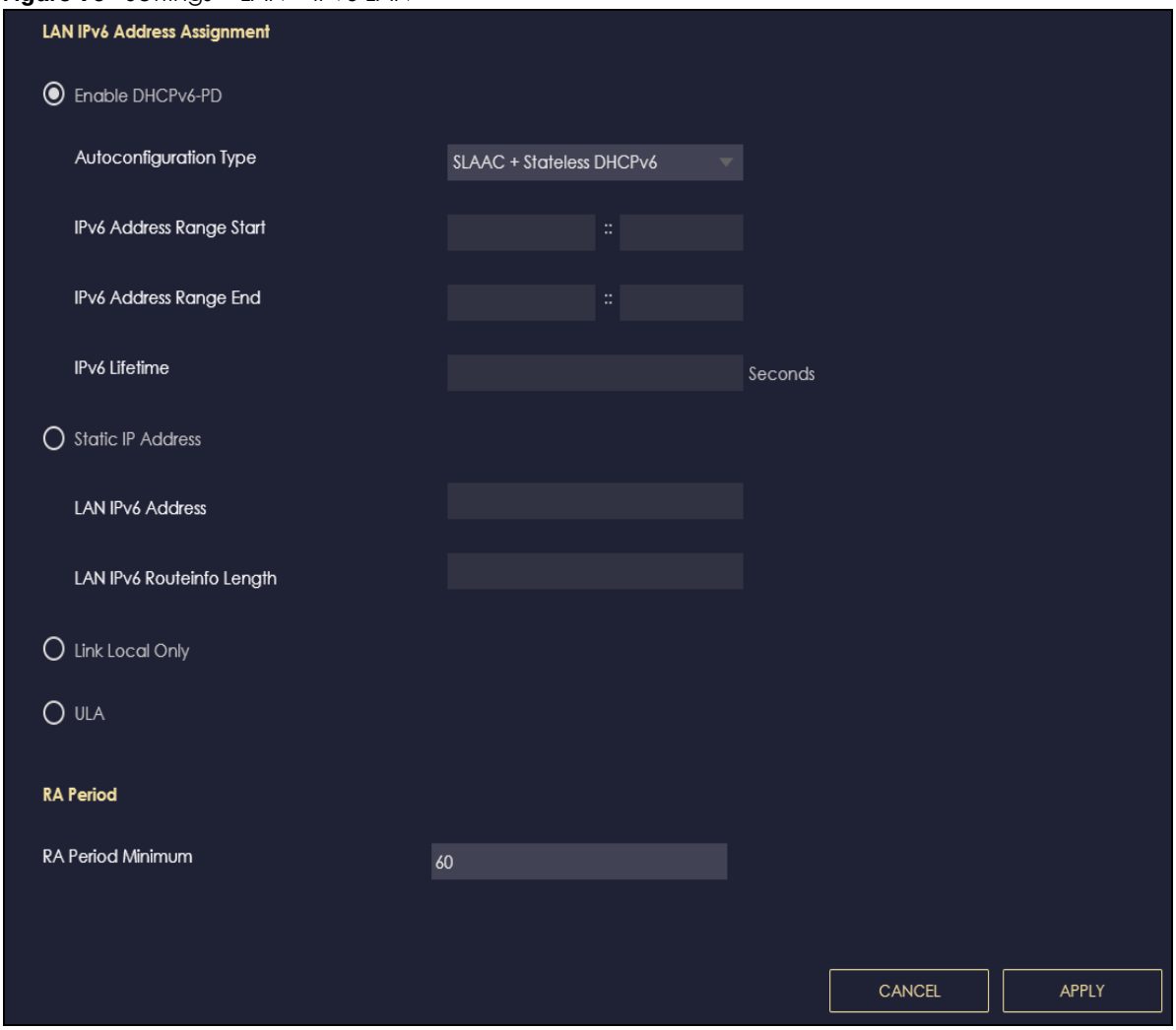
LABEL	DESCRIPTION
IP Address setting	
Obtain an IP Address Automatically (DHCP)	When you enable this, the NBG6818 gets its IP address from the network's DHCP server (for example, your ISP). Users connected to the NBG6818 can now access the network (i.e., the Internet if the IP address is given by the ISP). The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the NBG6818. You need to reset the NBG6818 to be able to access the Web Configurator again (see Section 13.6 on page 140 for details on how to reset the NBG6818). Also when you select this, you cannot enter an IP address for your NBG6818 in the field below.
Static IP Address	Click this if you want to specify the IP address of your NBG6818. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Enter the IP address in dotted decimal notation. The default setting is 192.168.1.2. If you change the IP address you will have to log in again with the new IP address.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG6818 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG6818.
Gateway	Enter a gateway IP address (if your ISP or network administrator gave you one) in this field.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the NBG6818's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **APPLY**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **APPLY**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
APPLY	Click **APPLY** to save your changes to the NBG6818.
CANCEL	Click **CANCEL** to reload the previous configuration for this screen.

11.5 IPv6 LAN Screen

Use this screen to configure the IP address for your NBG6818 on the LAN. Click **Settings** > **LAN** > **IPv6 LAN** to show the following screen.

Note: This is not available if you are using bridge mode.

Figure 76 Settings > LAN > IPv6 LAN



The following table describes the labels in this screen.

Table 44 Settings > LAN > IPv6 LAN

LABEL	DESCRIPTION
LAN IPv6 Address Assignment	
Enable DHCPv6-PD Select this option to use DHCPv6 prefix delegation. The NBG6818 will obtain an IPv6 prefix from the ISP or a connected uplink router for the LAN.	
Autoconfiguration Type	Select **SLAAC + RDNSS** to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network. Select **SLAAC + Stateless DHCPv6** to enable IPv6 stateless auto-configuration on this interface. The interface will get an IPv6 address from an IPv6 router and the DHCP server. The IP address information gets through DHCPv6. Select **Stateful DHCPv6** to allow a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients.
IPv6 Address range (Start)	Enter the beginning of the range of IP addresses that this address object represents.

Table 44 Settings > LAN > IPv6 LAN (continued)

LABEL	DESCRIPTION
IPv6 Address range (End)	Enter the end of the range of IP address that this address object represents.
IPv6 Lifetime	Enter the IPv6 lifetime in the LAN.
Static IP Address Select this option to manually enter an IPv6 address if you want to use a static IP address.	
LAN IPv6 Address	Enter the LAN IPv6 address you want to assign to your NBG6818 in hexadecimal notation.
LAN IPv6 Routeinfo Length (48~64)	Enter the 48 to 64 address prefix length to specify in an IPv6 address compose the network address.
Prefix Valid Lifetime	Enter the valid lifetime for the prefix.
Link Local Only Select this option to only use the link local address on the NBG6818 interfaces in the LAN.	
ULA Select this option to identify a unique local address of the NBG6818 in the LAN.	
RA period	
Minimum RA period	Enter the minimum time in seconds between router advertisement messages.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

CHAPTER 12
Security

12.1 Overview

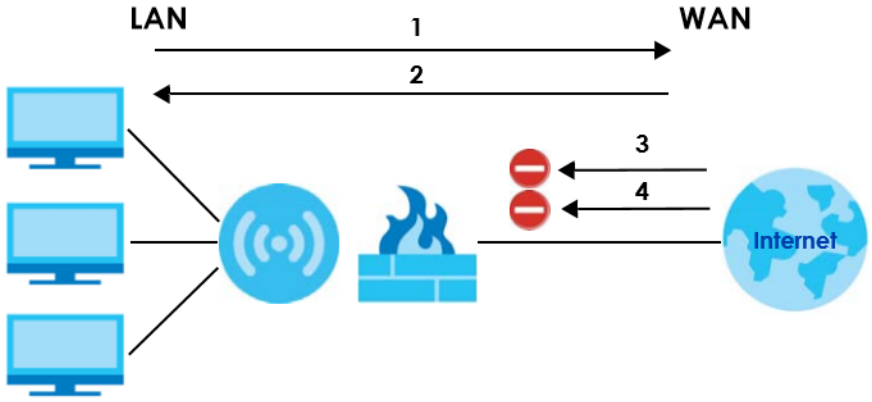
Use these screens to enable and configure the firewall that protects your NBG6818 and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 77 Default Firewall Action



Note: Features in this chapter are not available if you are using bridge mode.

12.1.1 What You Can Do

- Use the **IPv4 Firewall** screen to enable or disable the NBG6818's IPv4 firewall (Section 12.2 on page 128).
- Use the **IPv6 Firewall** screen to enable or disable the NBG6818's IPv6 firewall (Section 12.3 on page 131).

12.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

About the NBG6818 Firewall

The NBG6818's firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **IPv4 Firewall** or **IPv6 Firewall** tab under **Security** and then click the **Enable Firewall** check box). The NBG6818's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG6818 can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The NBG6818 is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The NBG6818 has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

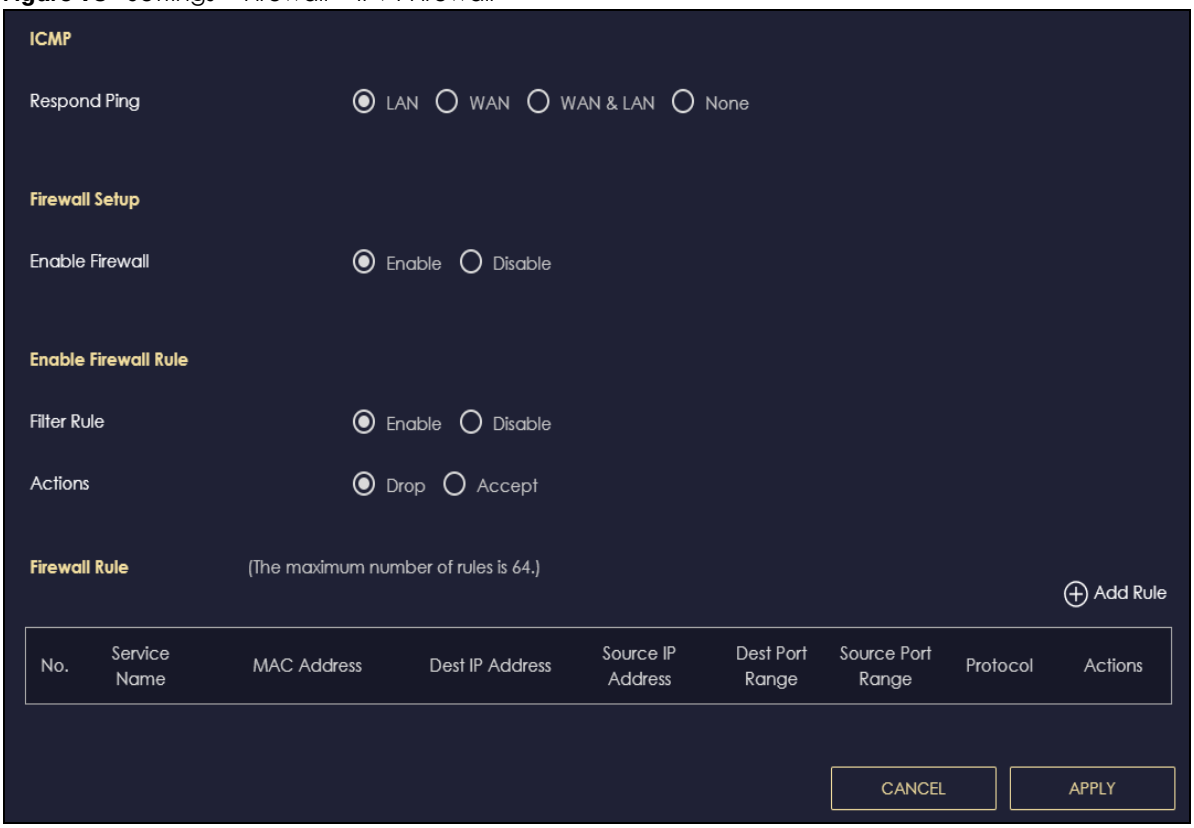
Guidelines For Enhancing Security With Your Firewall

1. Change the default password via Web Configurator.
2. Think about access control before you connect to the network in any way, including attaching a modem to the port.
3. Limit who can access your router.
4. Don't enable any local service (such as NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

12.2 IPv4 Firewall Screen

Use this screen to enable or disable the NBG6818's IPv4 firewall. Click **Settings** > **Firewall** > **IPv4 Firewall** to show the following screen.

Figure 78 Settings > Firewall > IPv4 Firewall



The following table describes the labels in this screen.

Table 45 Settings > Firewall > IPv4 Firewall

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The NBG6818 will not respond to any incoming Ping requests when **None** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN&WAN** to reply to all incoming LAN and WAN Ping requests.
Firewall Setup	
Enable Firewall	Select **Enable** to activate the firewall. The NBG6818 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Enable Firewall Rule	
Filter Rule	Select **Enable** to activate the firewall rules that you define (see Add Firewall Rule below).
Actions	Select **Drop** to silently discard the packets which meet the firewall rules. The others are accepted. Select **Accept** to allow the passage of the packets which meet the firewall rules. The others are blocked.
Firewall Rule	
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC address	This is the MAC address of the computer for which the firewall rule applies.

Table 45 Settings > Firewall > IPv4 Firewall (continued)

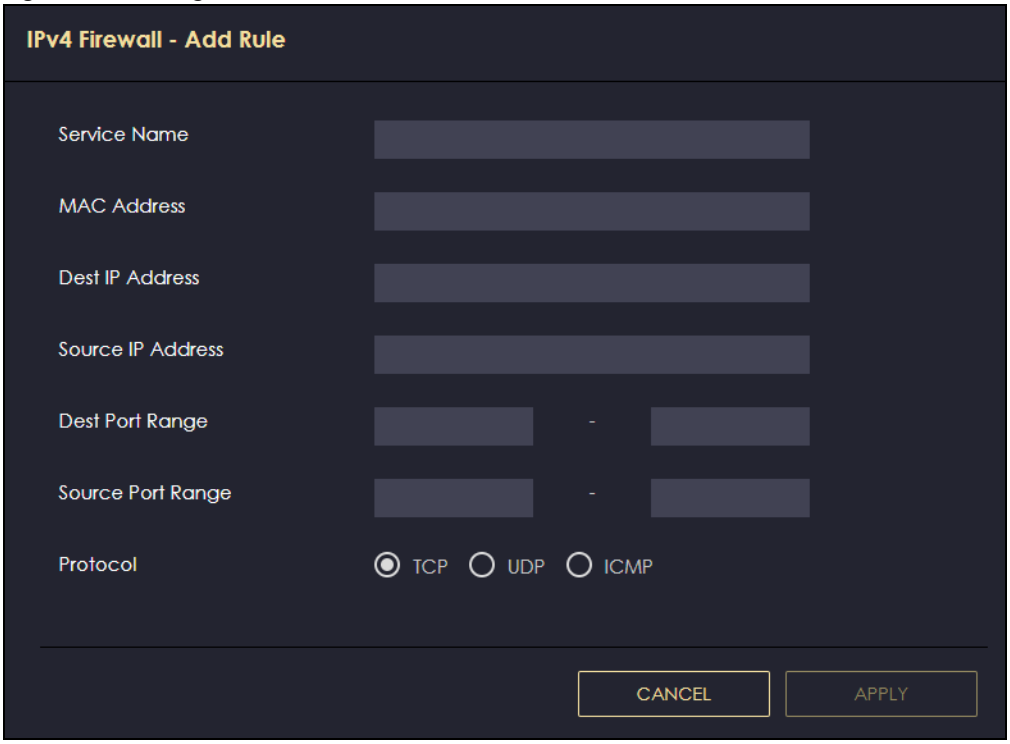
LABEL	DESCRIPTION
Dest IP Address	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP Address	This is the IP address of the computer from which traffic for the application or service is initialized.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 25 defines SMTP traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 25 defines SMTP traffic.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Actions	Click to remove the firewall rule. Click to edit the firewall rule.
APPLY	Click **APPLY** to save the settings.
CANCEL	Click **CANCEL** to start configuring this screen again.

12.2.1 IPv4 Firewall-Add Rule Screen

Use this screen to configure IPv4 firewall rule. Click **Add Rule** in the **Settings** > **Firewall** > **IPv4 Firewall** screen to open the following screen.

Note: For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website.

Figure 79 Settings > Firewall > IPv4 Firewall: Add Rule



The following table describes the labels in this screen.

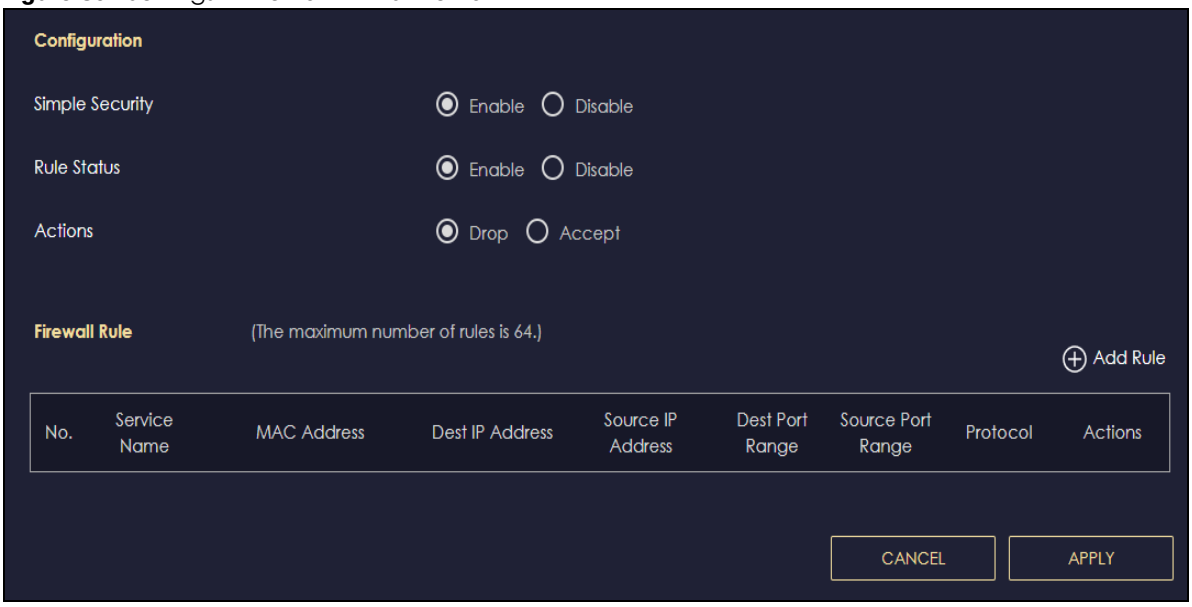
Table 46 Settings > Firewall > IPv4 Firewall: Add Rule

LABEL	DESCRIPTION
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The NBG6818 applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The NBG6818 applies the firewall rule to traffic initiating from this computer.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 25 defines SMTP traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 25 defines SMTP traffic.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
APPLY	Click **Apply** to save the settings.
CANCEL	Click **CANCEL** to exit this screen without saving.

12.3 IPv6 Firewall Screen

Use this screen to enable and create IPv6 firewall rules to filter IPv6 traffic. Click **Settings** > **Firewall** > **IPv6 Firewall** to show the following screen.

Figure 80 Settings > Firewall > IPv6 Firewall



The following table describes the labels in this screen.

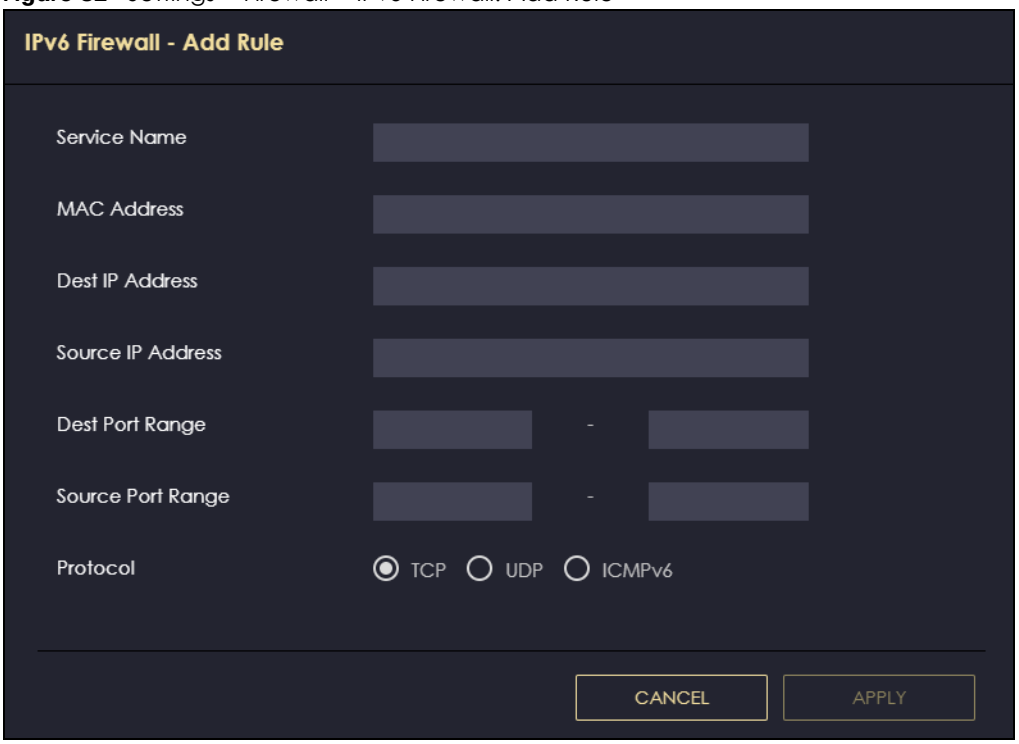
Table 47 Settings > Firewall > IPv6 Firewall

LABEL	DESCRIPTION
Configuration	
Simple Security	Select **Enable** to enabled simple security on your NBG6818.
Rule Status	Select **Enable** to enabled rule status on your NBG6818.
Action	Select **DROP** to silently discard the packets which meet the firewall rules. The others are accepted. Select **ACCEPT** to allow the passage of the packets which meet the firewall rules. The others are blocked.
Firewall Rule	
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC Address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP Address	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP Address	This is the IP address of the computer to which traffic for the application or service is initialized.
Dest Port Range	This is the port number/range of the destination that defines the traffic type, for example TCP port 25 defines SMTP traffic.
Source Port Range	This is the port number/range of the source that defines the traffic type, for example TCP port 25 defines SMTP traffic.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMPv6**) used to transport the packets for which you want to apply the firewall rule.
Actions	Click  to remove the firewall rule. Click  to edit the firewall rule.
APPLY	Click **APPLY** to save the settings.
CANCEL	Click **CANCEL** to restore your previously saved settings.

12.3.1 IPv6 Firewall-Add Rule Screen

Use this screen to configure IPv4 firewall rule. Click **Add Rule** in the **Settings** > **Firewall** > **IPv6 Firewall** screen to open the following screen.

Figure 81 Settings > Firewall > IPv6 Firewall: Add Rule



The following table describes the labels in this screen.

Table 48 Settings > Firewall > IPv4 Firewall: Add Rule

LABEL	DESCRIPTION
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The NBG6818 applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The NBG6818 applies the firewall rule to traffic initiating from this computer.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 25 defines SMTP traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 25 defines SMTP traffic.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
APPLY	Click **APPLY** to save the settings.
CANCEL	Click **CANCEL** to exit this screen without saving.

CHAPTER 13
System

13.1 Overview

This chapter provides information on checking the NBG6818's status and logs, configuring basic and remote management settings, using maintenance and firmware upgrade tools, and changing the operating mode.

13.2 What You Can Do

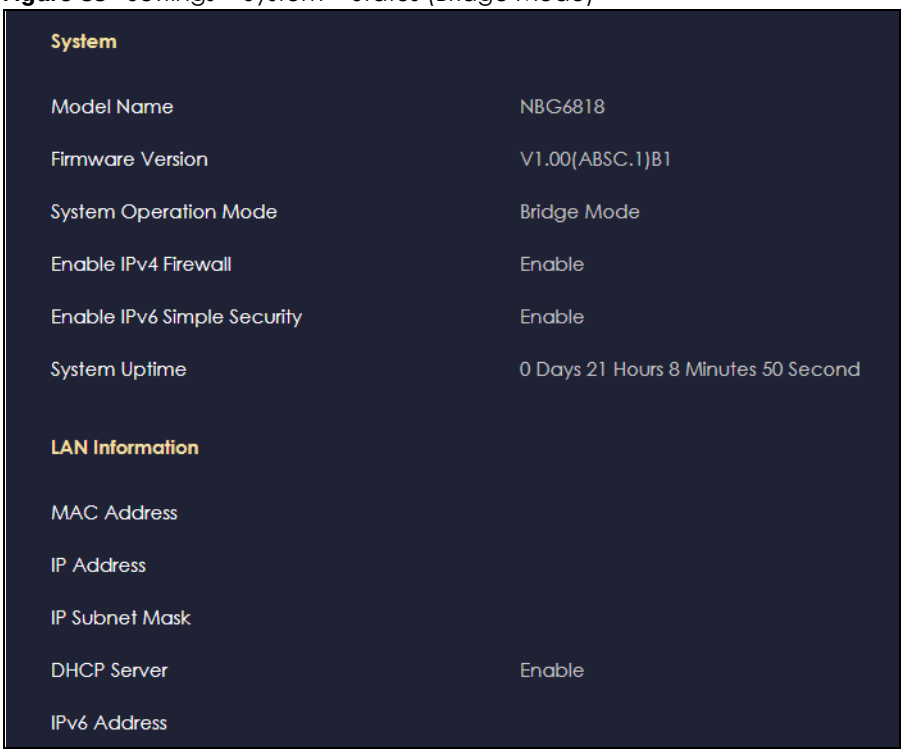
- Use the **Status** screen to view the basic information of the NBG6818 (Section 13.3 on page 134).
- Use the **General Setting** screen to change password or to set the timeout period of the management session (Section 13.4 on page 137).
- Use the **Remote Access** screen to configure the interface/s from which the NBG6818 can be managed remotely and specify a secure client that can manage the NBG6818 (Section 13.5 on page 139).
- Use the **Maintenance** screen to upload firmware, reboot the NBG6818 without turning the power off or reset the NBG6818 to factory defaults (Section 13.6 on page 140).
- Use the **Operating Mode** screen select whether you want the NBG6818 to act as a router or a bridge (Section 13.7 on page 141).
- Use the **Logs** screen to see the system logs recorded by the NBG6818 (Section 13.8 on page 142).

13.3 Status Screen

Use this screen to view some basic information of your NBG6818. Click **Settings** > **System** > **Status** to show the following screen.

Figure 82 Settings > System > Status (Standard Mode)

Figure 83 Settings > System > Status (Bridge Mode)



The following table describes the labels in this screen.

Table 49 Settings > System > Status

LABEL	DESCRIPTION
System	
Model Name	This is the model name of your device.
Firmware Version	This is the firmware version.
System Operation Mode	This is the device mode in which the NBG6818 is currently running. See Section 13.7 on page 141 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the NBG6818.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the NBG6818.
System Uptime	This is the total time the NBG6818 has been on.
WAN Information Note: : This is not available if you are using bridge mode.	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
IP Address	This shows the NBG6818's WAN IP address.
IP Subnet Mask	This shows the NBG6818's WAN subnet mask.
Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the current IPv6 address of the NBG6818.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the NBG6818's LAN IP address.
IP Subnet Mask	This shows the NBG6818's LAN subnet mask.

Table 49 Settings > System > Status (continued)

LABEL	DESCRIPTION
DHCP Server	This shows whether the NBG6818 acts as a DHCP Server and provides LAN IP addresses to its clients or not.
IPv6 Address	This shows the current LAN IPv6 address of the NBG6818.

13.4 General Setting Screen

Use this screen to set the management session timeout period. Click **Settings** > **System** > **General Setting** to show the following screen.

Figure 84 Settings > System > General Setting (Standard Mode)

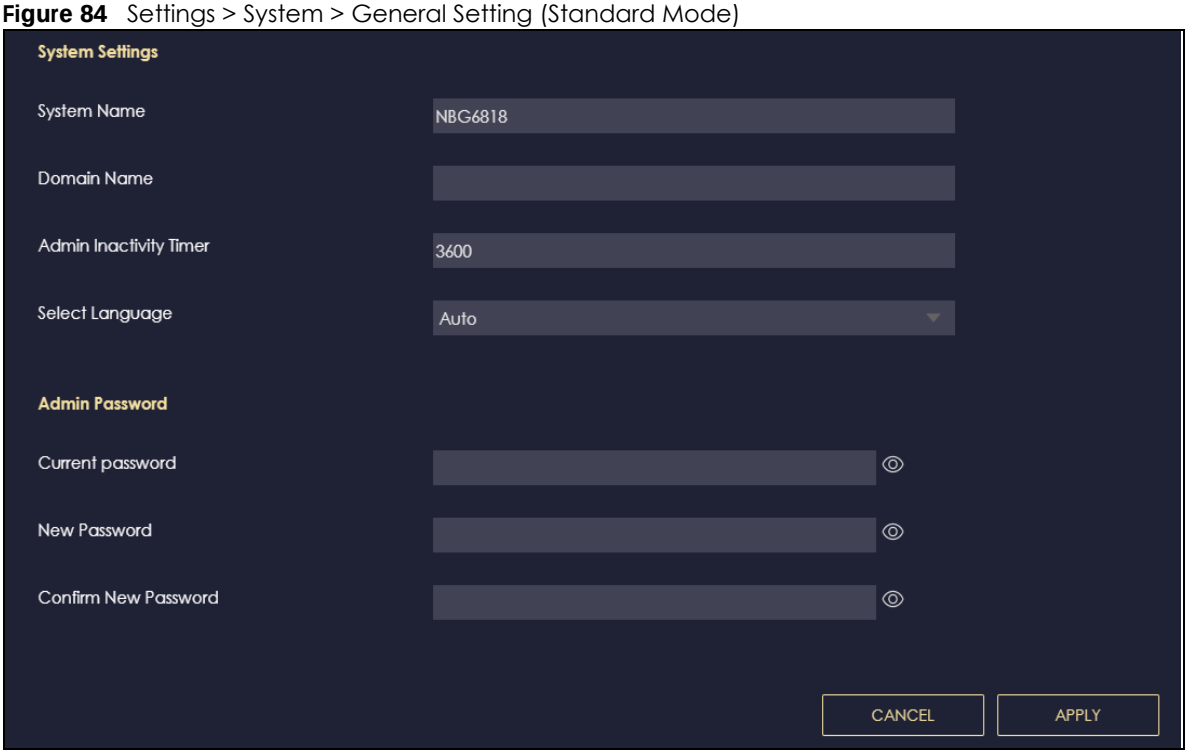
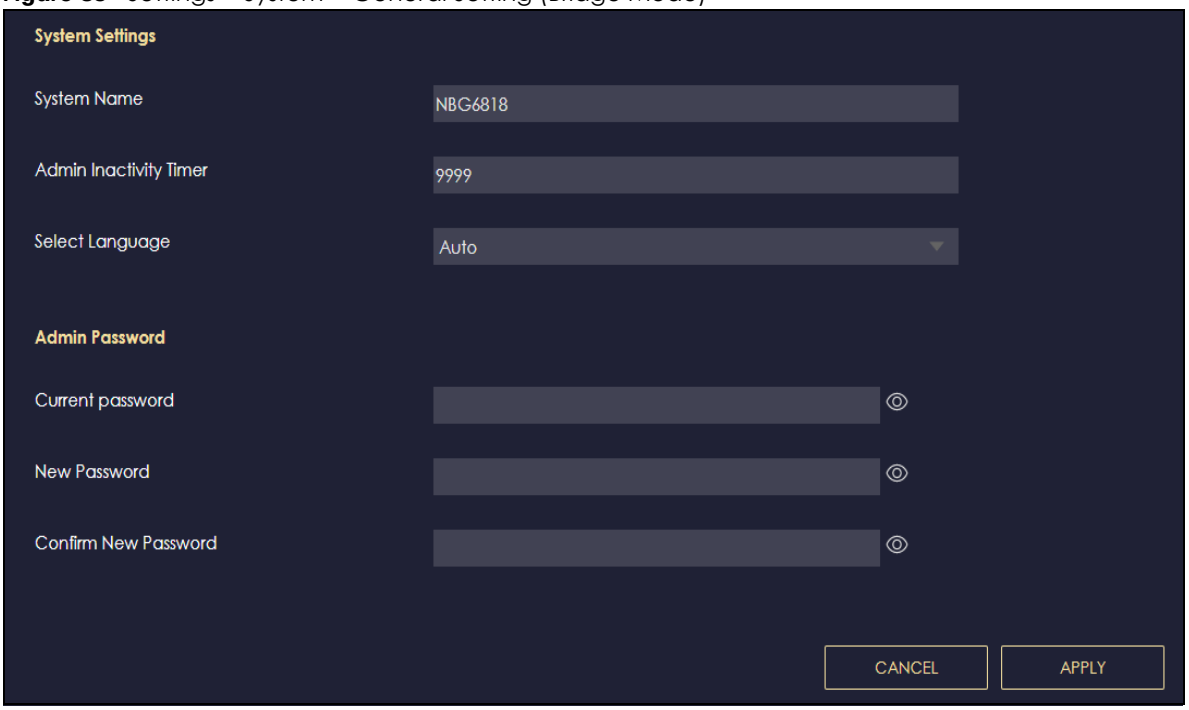


Figure 85 Settings > System > General Setting (Bridge Mode)



The following table describes the labels in this screen.

Table 50 Settings > System > General Setting

LABEL	DESCRIPTION
System Settings	
System Name	System Name is a unique name to identify the NBG6818 in an Ethernet network.
Domain Name (This is not available if you are using bridge mode)	Enter the domain name you want to give to the NBG6818.
Admin Inactivity Timer	Enter how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out, you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Select Language	Select a language you prefer from the drop-down list box. The Web Configurator language changes after a while without restarting the NBG6818.
Admin Password	
Current Password	Enter the default password or the existing password you use to access the system in this field.
New Password	Enter your new system password (up to 30 characters). Note that as you enter a password, the screen displays a dot for each character you enter.
Confirm New Password	Enter the new password again in this field.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to discard all changes.

13.5 Remote Access Screen

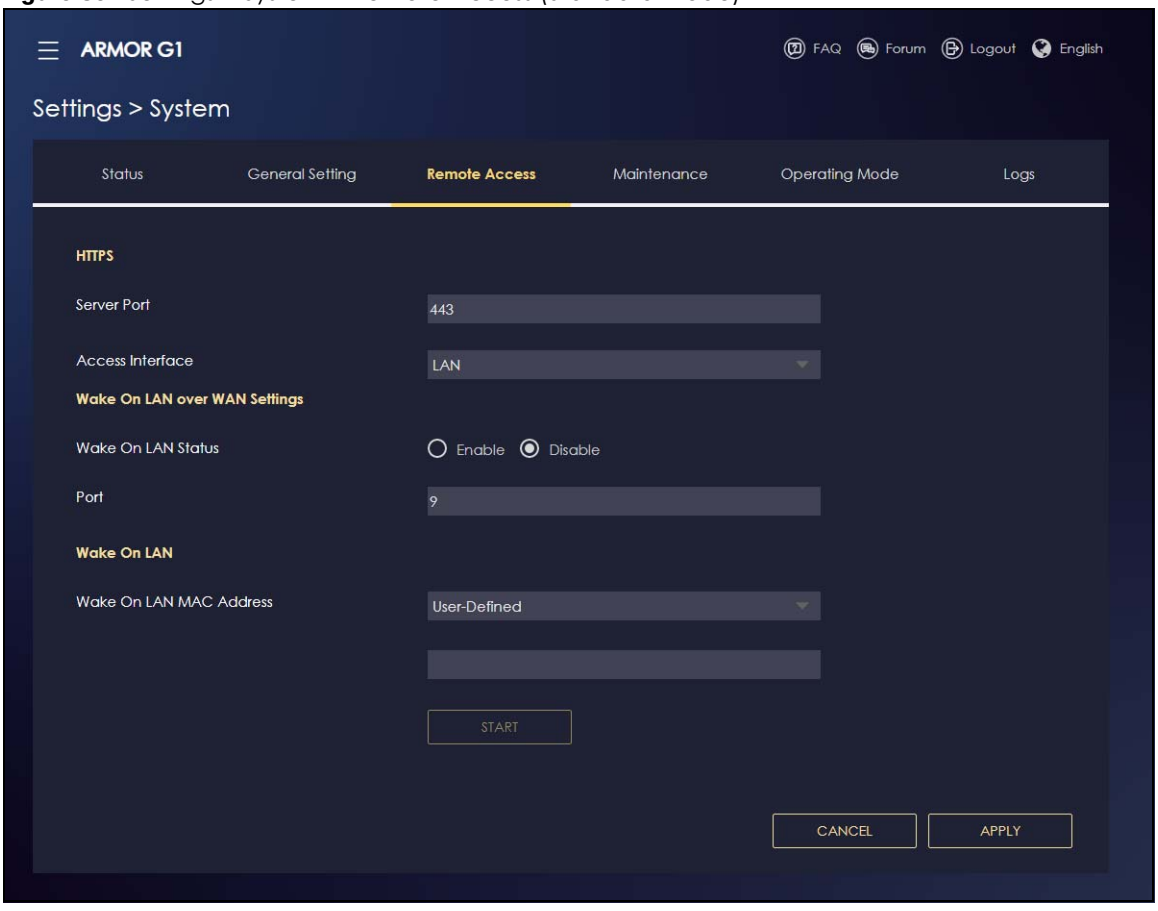
Use this screen to change your NBG6818's remote management settings. You can use HTTPS or Wake on LAN to access and manage the NBG6818.

Wake On LAN (WoL) allows you to remotely turn on a device on the network, such as a computer, storage device or media server. To use this feature, the remote hardware (such as the network adapter on a computer) must support Wake On LAN using the "Magic Packet" method.

You need to know the MAC address of the remote client to use this feature. It may be on a label on the device.

Click **Settings** > **System** > **Remote Access** to show the following screen.

Figure 86 Settings > System > Remote Access (Standard Mode)



The following table describes the labels in this screen.

Table 51 Settings > System > Remote Access

LABEL	DESCRIPTION
HTTPS	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Interface	Select the interface(s) through which a computer may access the NBG6818 using this service.

Table 51 Settings > System > Remote Access (continued)

LABEL	DESCRIPTION
Wake on LAN	
Wake on LAN Status	Select **Enable** to have the NBG6818 forward a WoL "Magic Packet" to all devices on the LAN if the packet comes from the WAN or remote network and uses the port number specified in the **Port** field. A LAN device whose hardware supports Wake on LAN then will be powered on if it is turned off previously.
Port	Enter a port number from which a WoL packet is forwarded to the LAN.
Wake on LAN MAC Address	This field displays the hostname and MAC address of the LAN device by default. Otherwise, select **User-Defined** to enter the MAC Address of the device on the network that will be turned on. A MAC address consists of six hexadecimal character pairs.
Start	Click this to have the NBG6818 generate a WoL packet and forward it to turn the specified device on. A screen pops up displaying MAC address error if you input the MAC address incorrectly.
APPLY	Click **APPLY** to save your changes back to the NBG6818.
CANCEL	Click **CANCEL** to begin configuring this screen afresh.

13.6 Maintenance Screen

Use this screen to upgrade firmware, restart or reset your NBG6818.

Online Firmware

Find firmware at www.zyxel.com in a file that uses the version number and project code with a "*.bin" extension, e.g., "V1.00(ABCS.0)C0.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

System Restart

System restart allows you to reboot the NBG6818 without turning the power off.

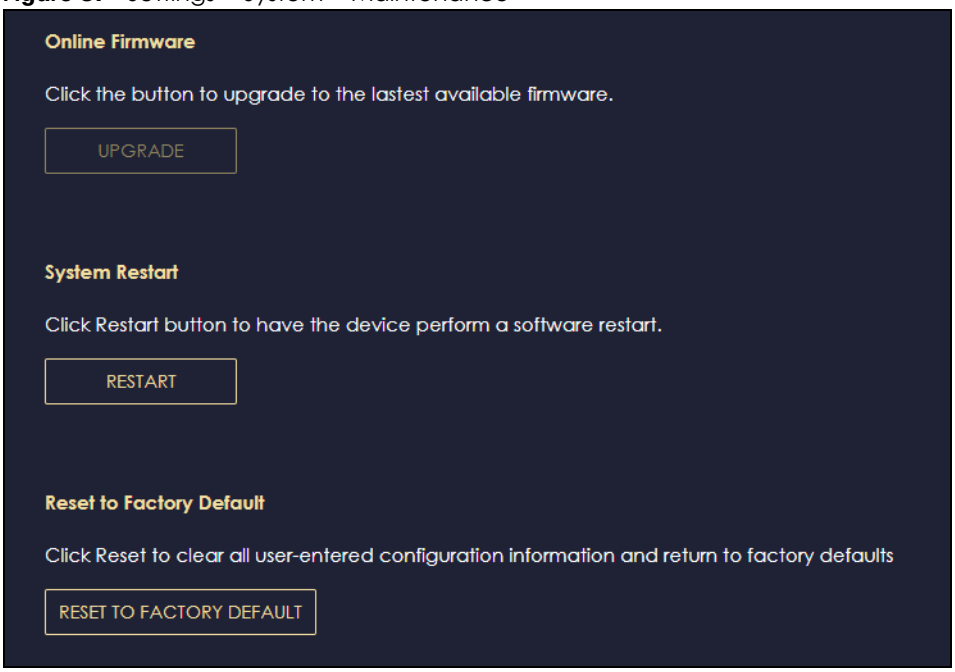
Reset to Factory Default

Click the **RESET TO FACTORY DEFAULT** button in this section to clear all user-entered configuration information and returns the NBG6818 to its factory defaults.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG6818.

Click **Settings** > **System** > **Maintenance** to show the following screen.

Figure 87 Settings > System > Maintenance



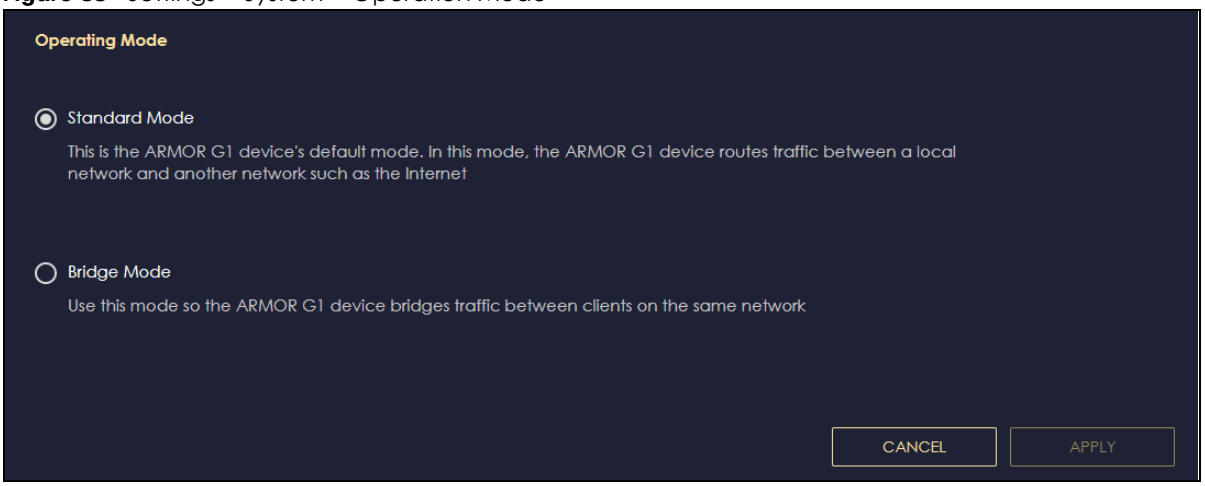
13.7 Operating Mode Screen

Use this screen to select how you want to use your NBG6818.

The **Operating Mode** function lets you configure your NBG6818 as a router or bridge. You can choose between **Standard Mode**, and **Bridge Mode** depending on your network topology and the features you require from your NBG6818.

Click **Settings** > **System** > **Operating Mode** to show the following screen.

Figure 88 Settings > System > Operation Mode



The following table describes the labels in this screen.

Table 52 Settings > System > Operation Mode

LABEL	DESCRIPTION
Standard Mode	Select **Standard Mode** if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or bandwidth management. You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.
Bridge Mode	Select Bridge Mode if your device bridges traffic between clients on the same network. • In Bridge Mode, all Ethernet ports have the same IP address. • All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port. • The DHCP server on your device is disabled. • Router functions (such as NAT, bandwidth management, remote management, firewall and so on) are not available when the NBG6818 is in Bridge Mode. • The IP address of the device on the local network is set to 192.168.123.2.
APPLY	Click **APPLY** to save your settings.
CANCEL	Click **CANCEL** to return your settings to the default (**Standard**).

Note: If you select the incorrect system operation Mode you may not be able to connect to the Internet

13.8 Logs Screen

Use this screen to see the logged messages for the NBG6818.

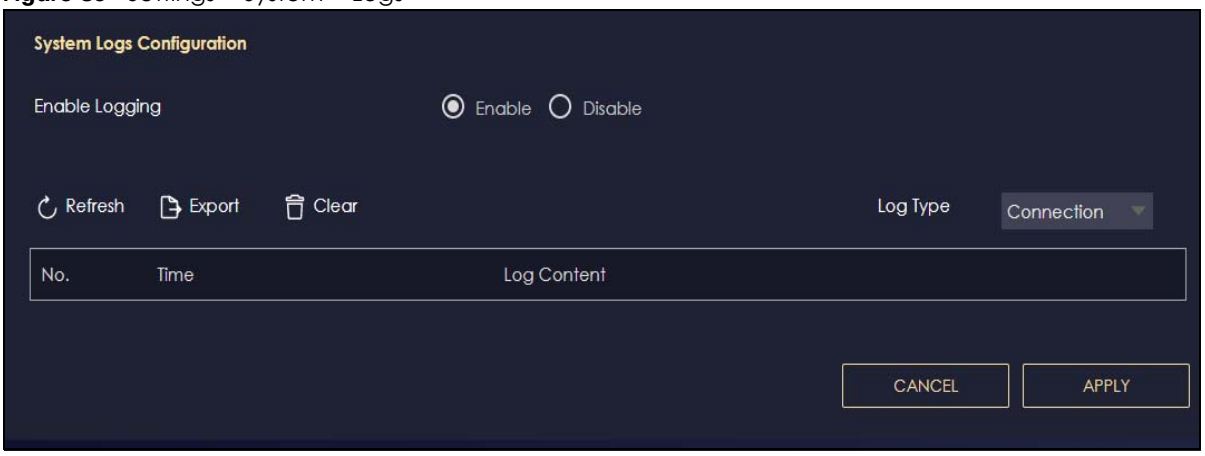
You can configure which logs to display in the Log screen.

The newest log replaces the oldest log after it fills. Select what logs you want to see from the **Log Type** drop-down list box. The log choices depend on your other settings in the **System** screens. Click **Refresh** to renew the log screen. Click **Export** to save the current list of logs to your computer. Click **Clear** to delete all the logs.

Click **APPLY** to save your settings. Click **CANCEL** to discard all changes.

Click **Settings** > **System** > **Logs** to show the following screen.

Figure 89 Settings > System > Logs



PART III
Troubleshooting and Appendices

Appendices contain general information. Some information may not apply to your NBG6818.

CHAPTER 14 Troubleshooting

14.1 Troubleshooting Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware connections, and LEDs
- NBG6818 Access and Login
- Internet Access
- Resetting the NBG6818 to Its Factory Defaults
- WiFi Connections
- OpenVPN Problems
- USB Device Problems

14.2 Power, Hardware connections, and LEDs

The NBG6818 does not turn on. None of the LEDs turn on.

- Make sure you are using the power adaptor or cord included with the NBG6818.
- Make sure the power adaptor or cord is connected to the NBG6818 and plugged in to an appropriate power source. Make sure the power source is turned on.
- Disconnect and re-connect the power adaptor or cord to the NBG6818.
- If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

- Make sure you understand the normal behavior of the LED.
- Check the hardware connections. See the Quick Start Guide.
- Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- Disconnect and re-connect the power adaptor to the NBG6818.
- If the problem continues, contact the vendor.

14.3 NBG6818 Access and Login

I don't know the IP address of my NBG6818.

- The default IP address of the NBG6818 in **Standard Mode** is **192.168.123.1**. If the NBG6818 obtains a WAN IP address in the same subnet as the LAN IP address 192.168.123.1, the default LAN IP address will be changed to 10.0.0.1 automatically. See Auto-IP Change on page 17 for more information.
  The default IP address of the NBG6818 in **Bridge Mode** is **192.168.123.2**.
- If you changed the IP address and have forgotten it, you might get the IP address of the NBG6818 in **Standard Mode** by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the NBG6818 (it depends on the network), so enter this IP address in your Internet browser.
- If your NBG6818 in **Bridge Mode** is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
- Reset your NBG6818 to change all settings back to their default. This means your current settings are lost. See Section 14.5 on page 148 in the **Troubleshooting** for information on resetting your NBG6818.

I cannot see or access the **Login** screen in the Web Configurator.

- Make sure you are using the correct IP address.
- The default IP address of the NBG6818 in **Standard Mode** is **192.168.123.1**. If the NBG6818 obtains a WAN IP address in the same subnet as the LAN IP address 192.168.123.1, the default LAN IP address will be changed to 10.0.0.1 automatically. See Auto-IP Change on page 17 for more information.
  The default IP address of the NBG6818 in **Bridge Mode** is **192.168.123.2**.
- If you changed the IP address (Section 11.4 on page 118), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my NBG6818.
- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix B on page 157 for more information.
- Make sure your computer is in the same subnet as the NBG6818. (If you know that there are routers between your computer and the NBG6818, skip this step.)
- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 11.4 on page 118.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG6818. See Section 11.4 on page 118.
- Reset the device to its factory defaults, and try to access the NBG6818 with the default IP address. See Section on page 19.
- If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG6818 using another service, such as Telnet. If you can access the NBG6818, check the remote management settings and firewall rules to find out why the NBG6818 does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the NBG6818.

- This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- Disconnect and re-connect the power adaptor or cord to the NBG6818.
- If this does not work, you have to reset the device to its factory defaults. See Section 14.5 on page 148.

14.4 Internet Access

I cannot access the Internet.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- Go to **Expert** > **Maintenance > Operation Mode**. Check your System Operation Mode setting.

  If the NBG6818 is in **Standard Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the NBG6818 should be in the same subnet.

  If the NBG6818 is in **Bridge Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
- If the NBG6818 is in **Standard Mode**, make sure you entered your ISP account information correctly in the wizard or the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- If you are trying to access the Internet wirelessly, make sure the WiFi settings in the WiFi client are the same as the settings in the AP.
- Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG6818), but my Internet connection is not available anymore.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Table 4 on page 21.
- Reboot the NBG6818.

- If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- There might be a lot of traffic on the network. Look at the LEDs, and check Table 4 on page 21. If the NBG6818 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- Check the signal strength. If the signal strength is low, try moving the NBG6818 closer to the AP if possible, and look around to see if there are any devices that might be interfering with the WiFi network (for example, microwaves, other WiFi networks, and so on).
- Reboot the NBG6818.
- If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

14.5 Resetting the NBG6818 to Its Factory Defaults

If you reset the NBG6818, you lose all of the changes you have made. The NBG6818 reloads its default settings. (for example, default Standard (Router) operation mode and login IP address of 192.168.123.1, WiFi SSID and password). You have to make all of your changes again. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the NBG6818:

- Make sure the power LED is on.
- Press the **RESET** button for one to four seconds to restart/reboot the NBG6818.
- Press the **RESET** button for longer than five seconds to set the NBG6818 back to its factory-default configurations.

  If the NBG6818 restarts automatically, wait for the NBG6818 to finish restarting, and log in to the Web Configurator.

  If the NBG6818 does not restart automatically, disconnect and reconnect the NBG6818's power. Then, follow the directions above again.

14.6 WiFi Connections

I cannot access the NBG6818 or ping any computer from the WiFi.

- Make sure the WiFi is enabled on the NBG6818.

- Make sure the WiFi adapter on your computer is working properly.
- Make sure the WiFi adapter installed on your computer is IEEE 802.11 compatible and supports the same WiFi standard as the NBG6818.
- Make sure your computer (with a WiFi adapter installed) is within the transmission range of the NBG6818.
- Check that both the NBG6818 and the WiFi adapter on your computer are using the same WiFi and WiFi security settings.
- Make sure traffic between the WiFi and the LAN is not blocked by the firewall on the NBG6818.
- Make sure you allow the NBG6818 to be remotely accessed through the WiFi interface. Check your remote management settings.

  See the chapter on Wireless LAN in the User's Guide for more information.

I cannot access the Web Configurator after I switched to Bridge Mode.

- When you change from **Standard Mode** to **Bridge Mode**, your computer must have an IP address in the range between "192.168.123.3" and "192.168.123.254".

The WiFi connection is slow or intermittent.

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other WiFi devices.

To optimize the speed and quality of your WiFi connection, you can:

- Move your WiFi device closer to the NBG6818 if the signal strength is low.
- Reduce WiFi interference that may be caused by other WiFi networks or surrounding wireless electronics such as cordless phones.
- Place the NBG6818 where there are minimum obstacles (such as walls and ceilings) between the NBG6818 and the WiFi client. Avoid placing the NBG6818 inside any type of box that might block WiFi signals.
- Reduce the number of WiFi clients connecting to the same NBG6818 simultaneously, or add additional NBG6818s if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the WiFi client is sending or receiving a lot of information, it may have too many programs open that use the Internet.
- Position the antennas for best reception. If the NBG6818 is placed on a table or floor, point the antennas upwards. If the NBG6818 is placed at a high position, point the antennas downwards. Try pointing the antennas in different directions and check which provides the strongest signal to the WiFi clients.

14.7 OpenVPN Problems

Client devices cannot connect to the NBG6818 server.

- Make sure the NBG6818 is in standard (router) mode.
- Make sure DDNS is enabled in the **Settings** > **Internet** > **Dynamic DNS** screen.
- Make sure the OpenVPN Server account is enabled in the **OpenVPN Server** > **OpenVPN Server** screen.
- Make sure **Advertise DNS to Clients** is enabled in **OpenVPN Server** > **OpenVPN Server** screen.
- Make sure the VPN client is using a reliable Internet connection.
- Make sure the VPN client is using the correct protocol (TCP/UDP) to connect to the OpenVPN Server.
- Make sure the client connecting to the OpenVPN Server account is using the same port number (default server port number is 1194) to access the server account.
- Make sure the "key" the VPN clients use to access the OpenVPN Server account is correct. If not, export the new .ovpn configuration file and send it to all OpenVPN clients so that they can use the new key.
- Disable any Internet security and antivirus software installed on the client device. Some Internet security and antivirus products are known to cause interference with VPN connections and should be disabled.

The NBG6818 client cannot connect to an OpenVPN server.

- Do NOT activate OpenVPN Server and OpenVPN Client at the same time on the NBG6818.
- Try to ping the OpenVPN server.
- Make sure connection to an OpenVPN Server account is enabled in the **OpenVPN Server** > **OpenVPN Client** screen.
- Make sure the interface through which the NBG6818 connects to an OpenVPN Server account is allowed in the **OpenVPN Server** > **OpenVPN Client** screen's **Enable VPN on** field.
- Make sure you enter the correct user name and password to connect to the OpenVPN Server account.

14.8 USB Device Problems

I cannot access or see a USB device that is connected to the NBG6818.

- Disconnect the problematic USB device, then reconnect it to the NBG6818.
- Ensure that the USB device has power.
- Check your cable connections.
- Restart the NBG6818 by disconnecting the power and then reconnecting it.

- If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the NBG6818 and try to connect to it again with your computer.
- If the problem persists, contact your vendor.

What kind of USB devices do the NBG6818 support?

- It is strongly recommended to use version 2.0 or higher USB storage devices (such as NTFS or FAT32 file system, USB hard drives) and/or USB devices. Other USB products are not guaranteed to function properly with the NBG6818.
- The NBG6818 do not support 3G/4G USB dongles.

APPENDIX A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

For Zyxel Communications offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Networks offices, see *https://www.zyxel.com/index.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd
- https://www.zyxel.com/in/en/

Kazakhstan

- Zyxel Kazakhstan
- https://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- https://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd
- https://www.zyxel.com/th/th/

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- https://www.zyxel.com/vn/vi

Europe

Belarus

- Zyxel BY
- https://www.zyxel.by

Bulgaria

- Zyxel България
- https://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- https://www.zyxel.com/cz/cs/

Denmark

- Zyxel Communications A/S
- https://www.zyxel.com/dk/da/

Finland

- Zyxel Communications
- https://www.zyxel.com/fi/fi/

France

- Zyxel France
- https://www.zyxel.fr

Germany

- Zyxel Deutschland GmbH
- https://www.zyxel.com/de/de/

Hungary

- Zyxel Hungary & SEE
- https://www.zyxel.com/hu/hu/

Italy

- Zyxel Communications Italy
- https://www.zyxel.com/it/it/

Netherlands

- Zyxel Benelux
- https://www.zyxel.com/nl/nl/

Norway

- Zyxel Communications
- https://www.zyxel.com/no/no/

Poland

- Zyxel Communications Poland
- https://www.zyxel.com/pl/pl/

Romania

- Zyxel Romania

- https://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

Spain

- Zyxel Communications ES Ltd
- https://www.zyxel.com/es/es/

Sweden

- Zyxel Communications
- https://www.zyxel.com/se/sv/

Switzerland

- Studerus AG
- https://www.zyxel.ch/de
- https://www.zyxel.ch/fr

Turkey

- Zyxel Turkey A.S.
- https://www.zyxel.com/tr/tr/

UK

- Zyxel Communications UK Ltd.
- https://www.zyxel.com/uk/en/

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

South America

Argentina

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Colombia

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Ecuador

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

South America

- Zyxel Communications Corporation
- https://www.zyxel.com/co/es/

Middle East

Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- https://www.zyxel.com/us/en/

APPENDIX B
Setting Up Your Computer's IP Address

Note: The NBG6818 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network.

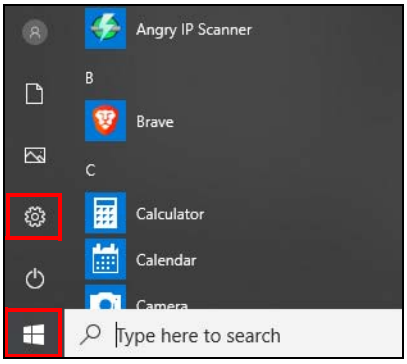
If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

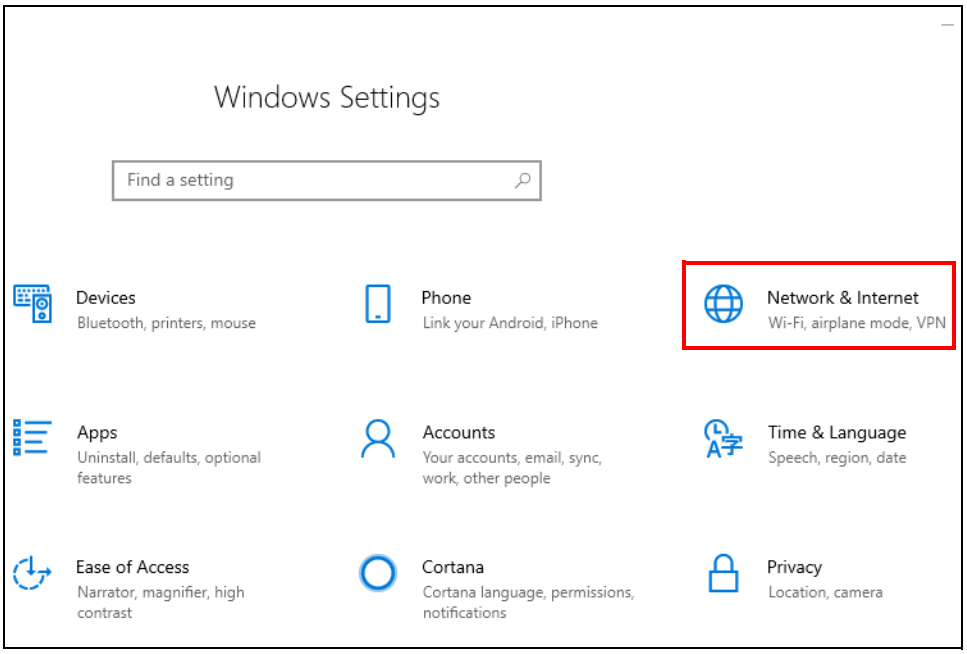
Windows 10

This section shows the screens from Windows 10 Professional.

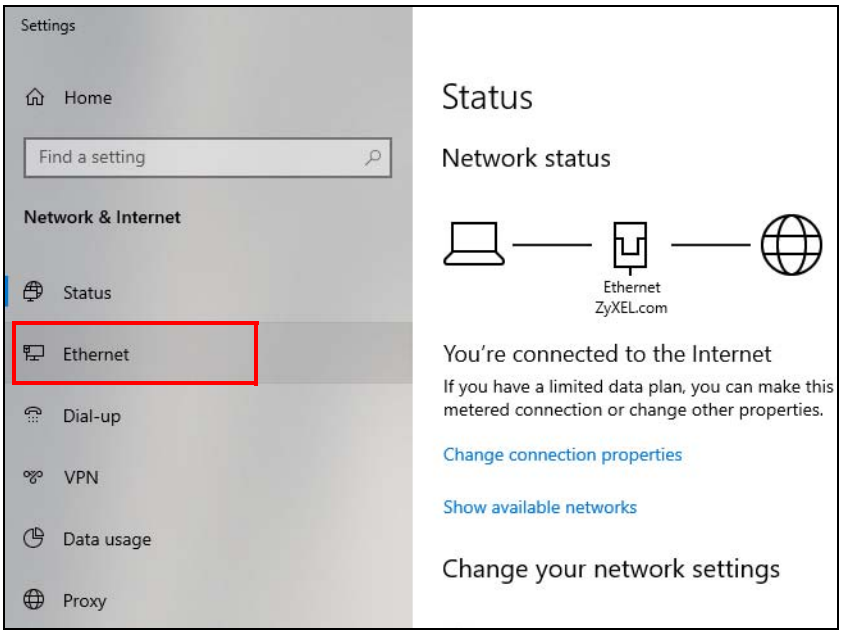
1 Click **Start** > **Settings** .



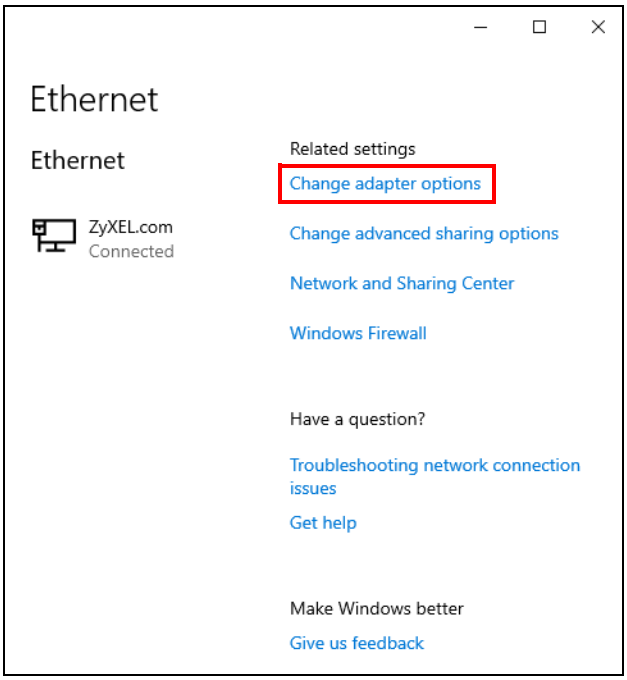
2 In the **Windows Settings** panel, click **Network & Internet**.



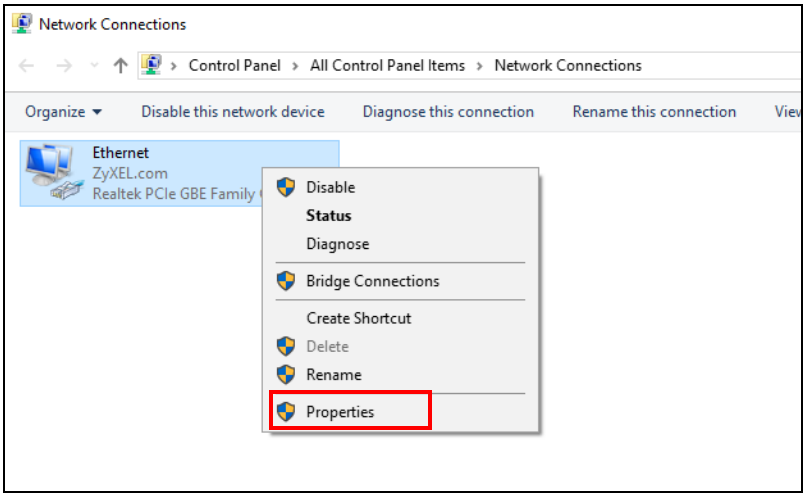
3 In the **Network & Internet** panel, click **Ethernet**.



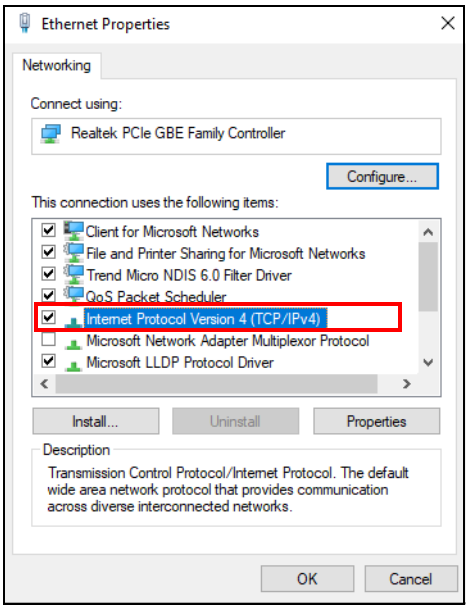
4 Click **Change adapter options**. The **Network Connections** panel opens.



5 Right-click the Ethernet network you are connected to, then select **Properties**.

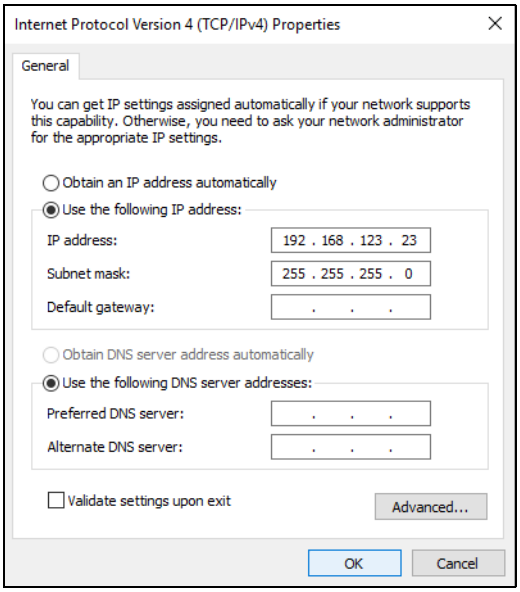


6 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens. Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Alternatively, select **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.



8 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

9 Click **OK** to close the **Ethernet Properties** window.

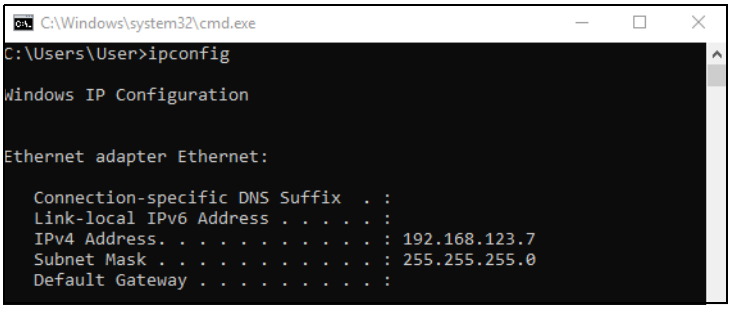
Verify the Settings

1 Use [Win] + [R] to open the **Run** window.

2 Enter "cmd" and click **OK** or press [ENTER] to open the **Command Prompt** window.

3 In the **Command Prompt** window, enter "ipconfig" and then press [ENTER].

4 The IP settings are displayed as follows.



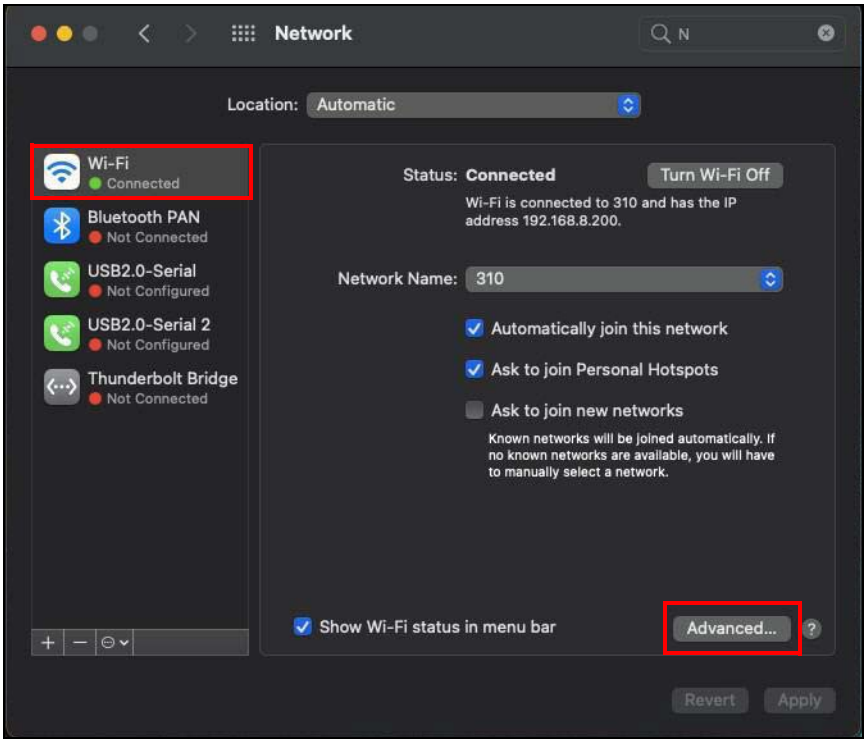
macOS: Big Sur 11

The screens in this section are from macOS Big Sur (v11).

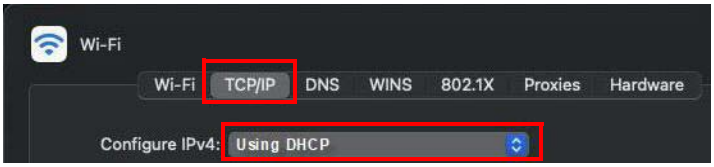
1 Click **Apple** > **System Preferences**.

2 In the **System Preferences** window, click the **Network** icon.

3 The **Network** preferences pane opens. Select the connection type you want to configure from the network connection type list, and then click **Advanced.** Here, we use **Wi-Fi** connection as an example**.**



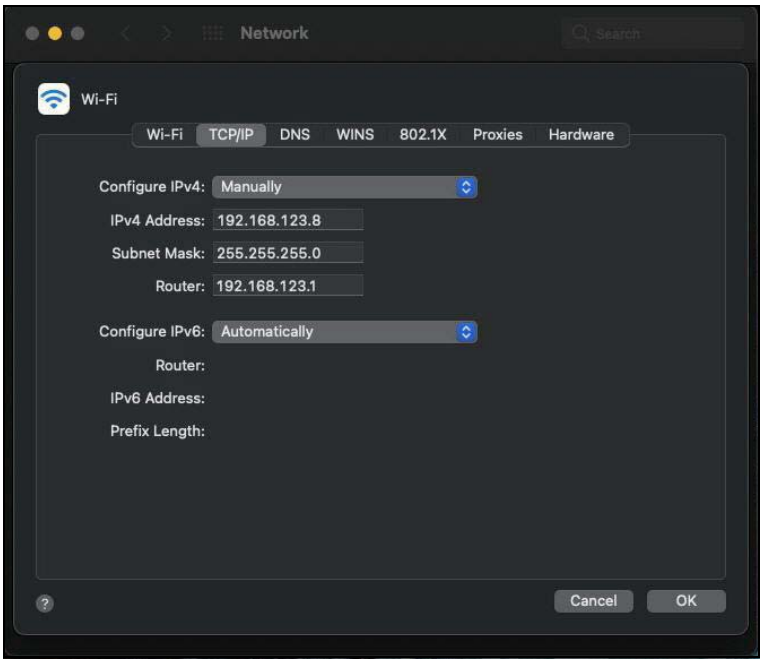
4 Select the **TCP/IP** tab to configure IP settings. For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list.



5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, enter your IP address.

- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your NBG6818.

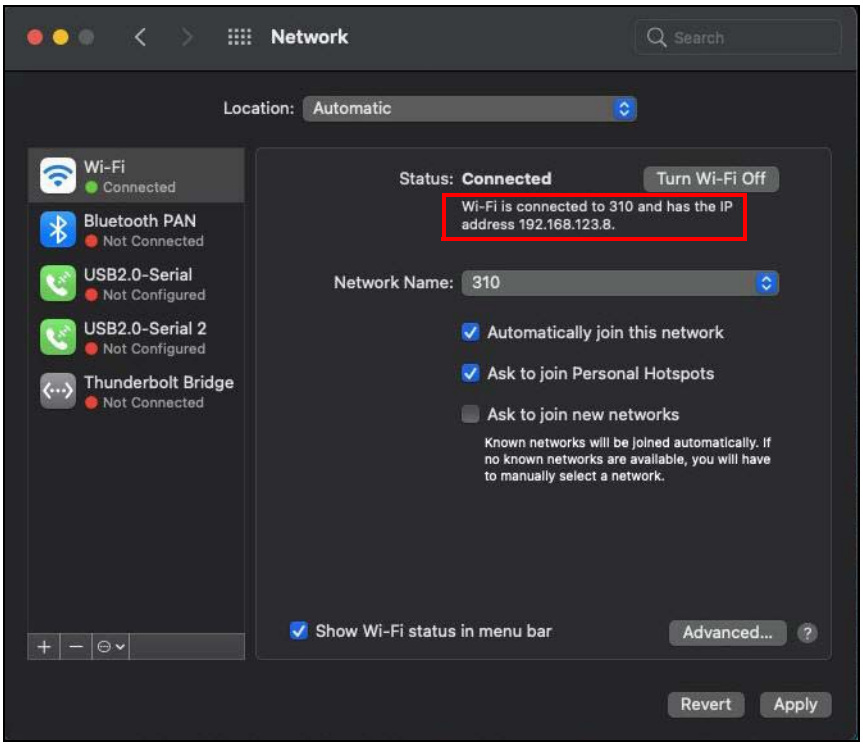


6 Click **OK**.

7 Click **Apply** on the **Network** panel to apply the settings.

Verify the Settings

Check your TCP/IP properties by clicking **Apple** > **System Preferences** > **Network**, and then selecting the appropriate connection type from the Internet connection list.



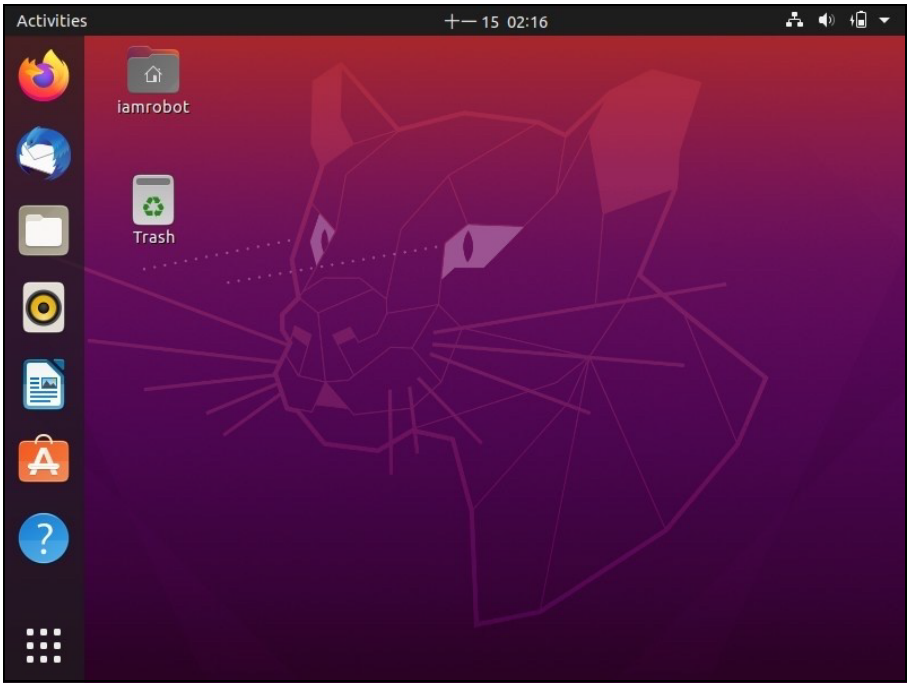
Linux: Ubuntu 20 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 20 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

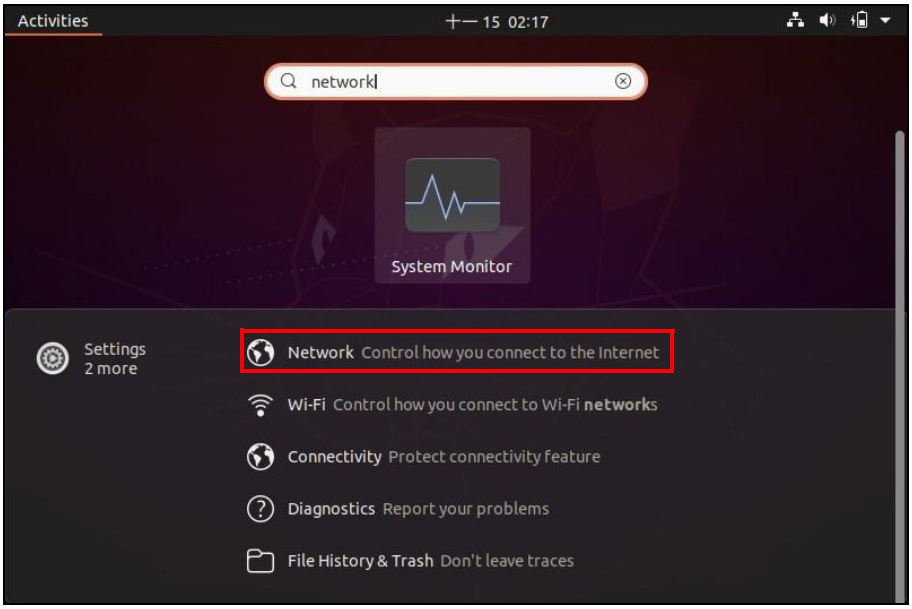
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer's IP address in GNOME:

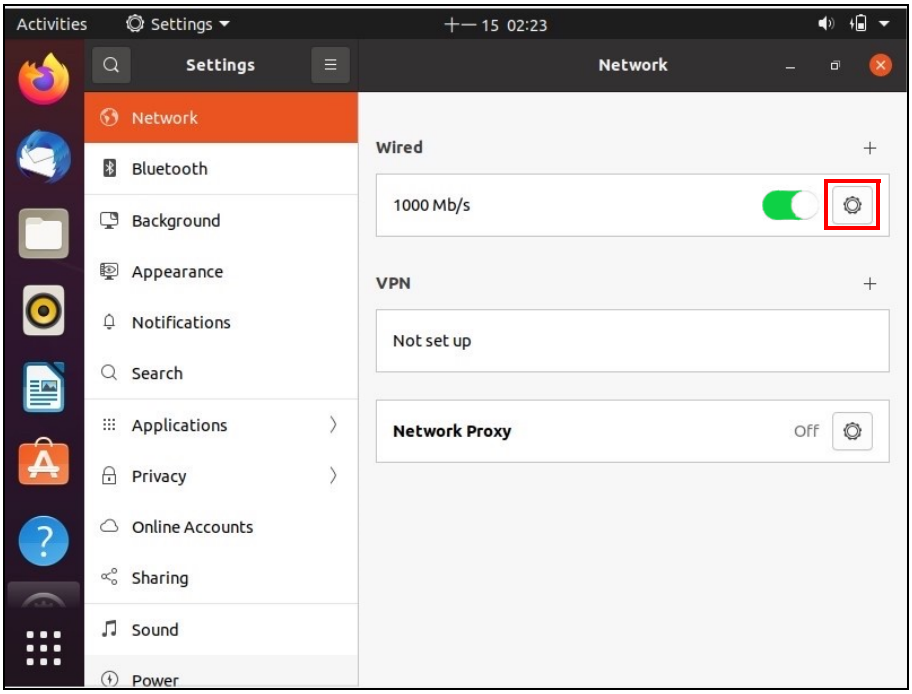
1 Click **Activities** (upper left) to open the search panel.



2 Enter "network" and the system will display the search results related to "network". Click **Network** to open the **Network** panel.

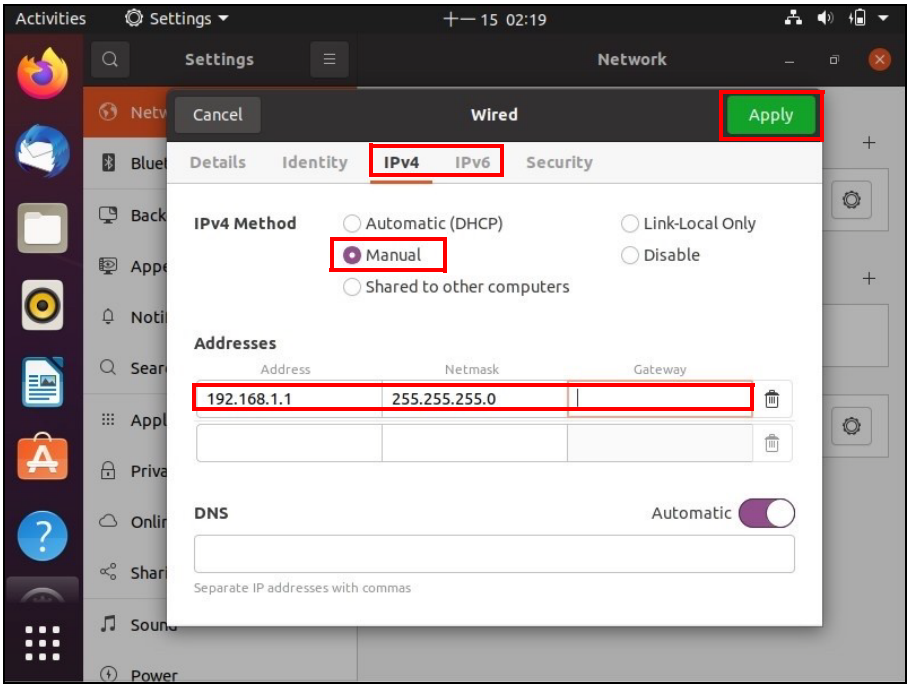


3 Click the settings icon  of the connection you want to configure.



4 Click the **IPv4** or **IPv6** tab to configure their settings. In this example, we select **IPv4**.

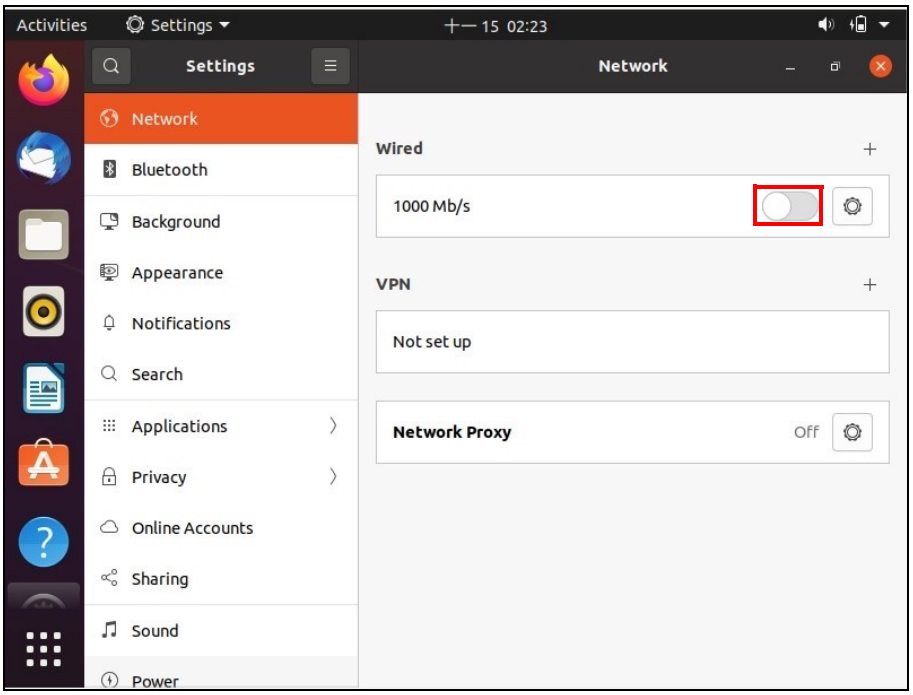
- Under **IPv4 Method**, select **Manual** if you have a static IP address. Fill in the IP **Address**, **Netmask**, and **Gateway** address fields. Enter the DNS settings if you know your DNS server IP addresses.
- Alternatively, select **Automatic (DHCP)** if you are assigned a dynamic IP address.



5 Click **Apply** to save the configuration.

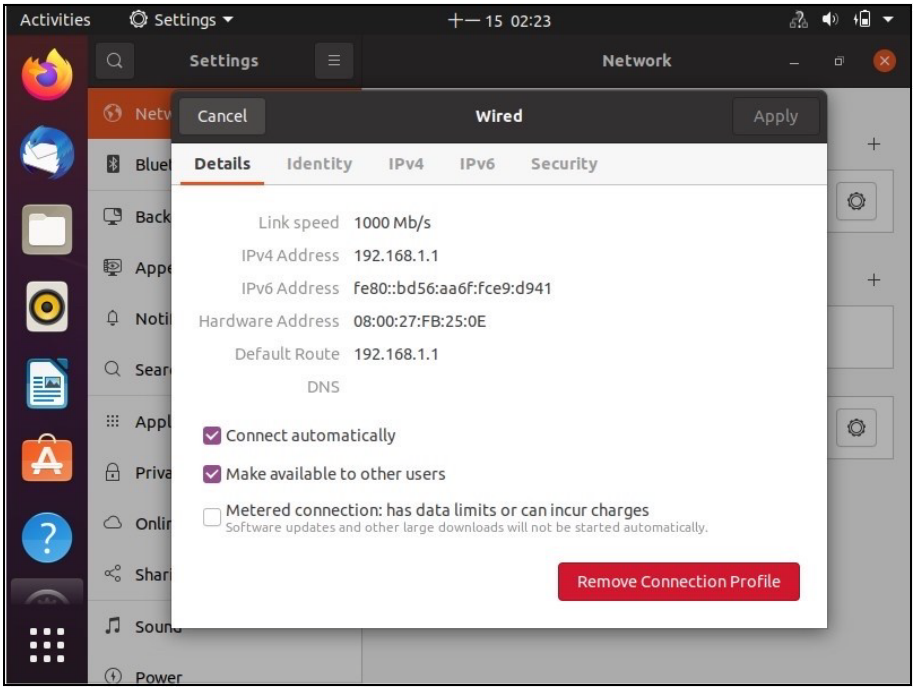
Note: The configuration will be applied after rebooting or connection interface restart.

6 To apply the configuration, click the switch to turn off and on to restart the connection interface.



Verify the Settings

Check your TCP/IP properties by opening the connection settings panel and selecting the **Details** tab.



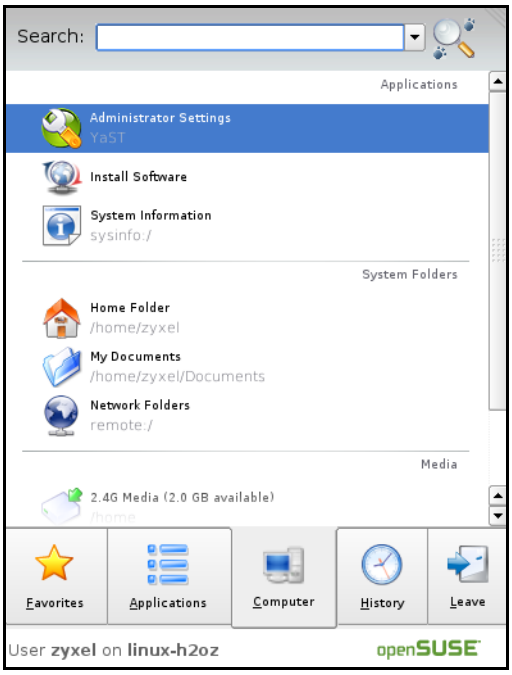
Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

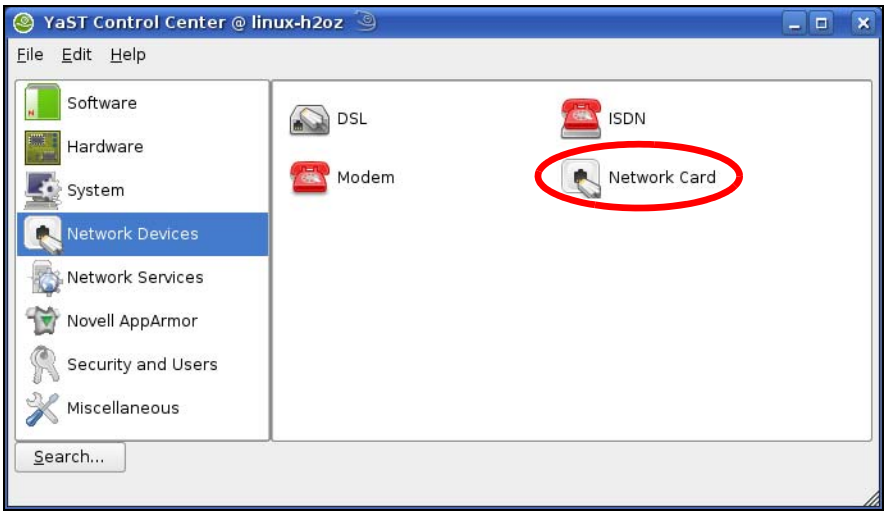
Follow the steps below to configure your computer's IP address in KDE:

1 Click **K Menu** > **Computer** > **Administrator Settings (YaST)**.

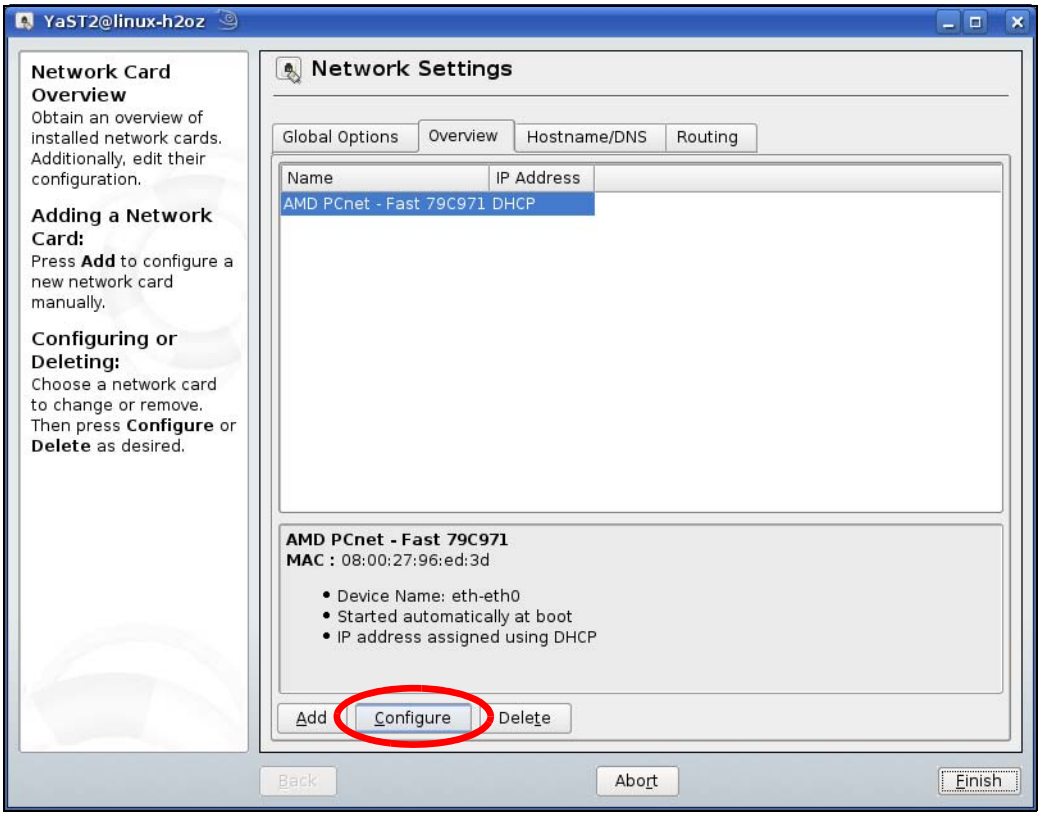


2 When the **Run as Root** – **KDE su** dialog opens, enter the **Administrator Password** and click **OK**.

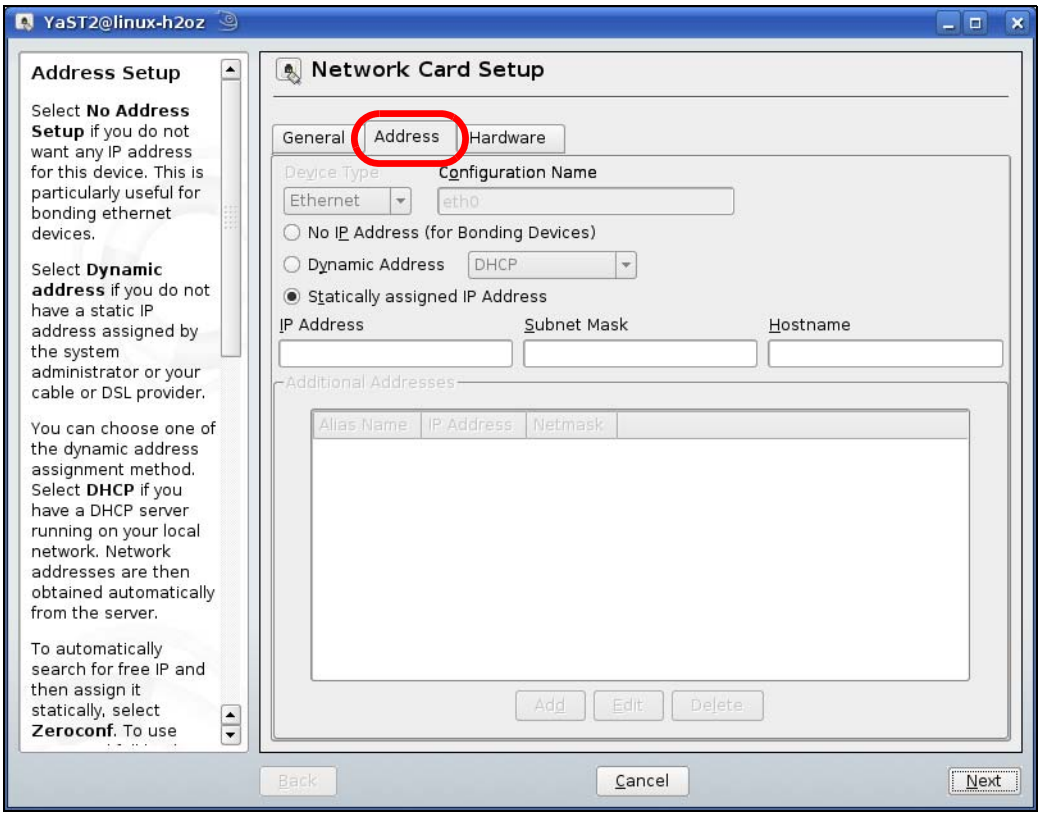
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.



4 When the **Network Settings** window opens, click the **Overview** tab. Select the appropriate connection **Name** from the list, and then click the **Configure** button.



5 When the **Network Card Setup** window opens, click the **Address** tab.

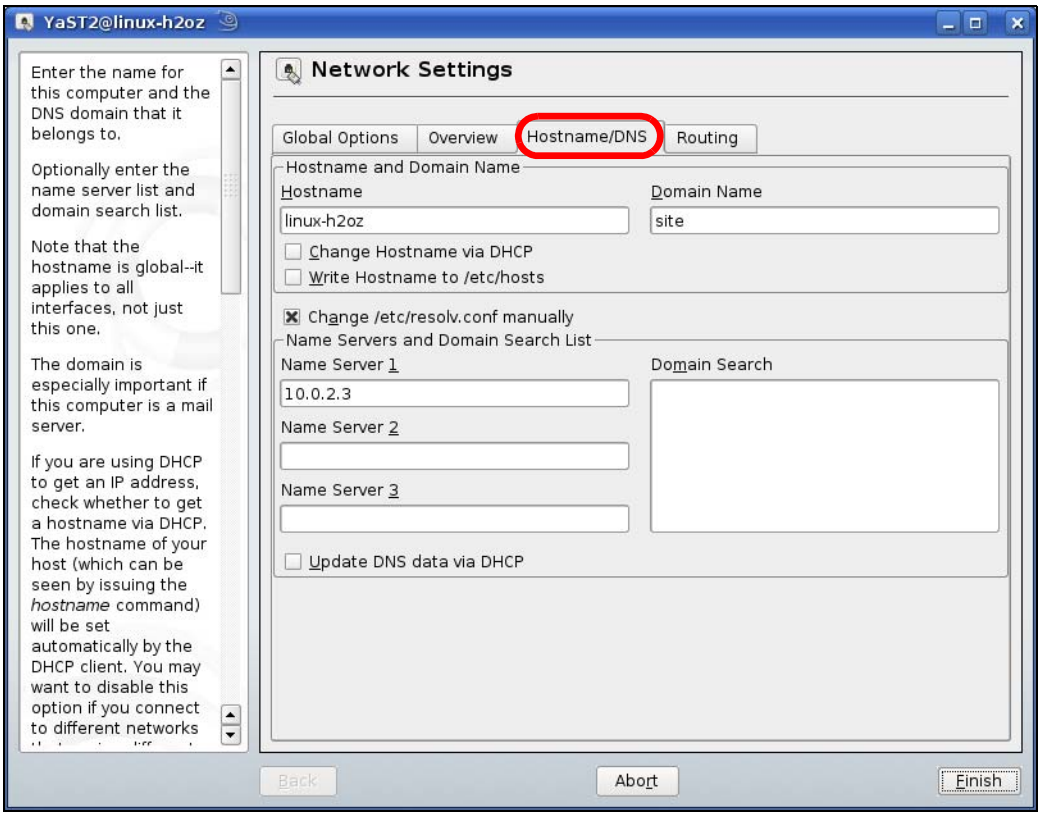


6 Select **Dynamic Address (DHCP)** if you are using a dynamic IP address.

Alternatively, select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP Address**, **Subnet Mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP addresses, click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

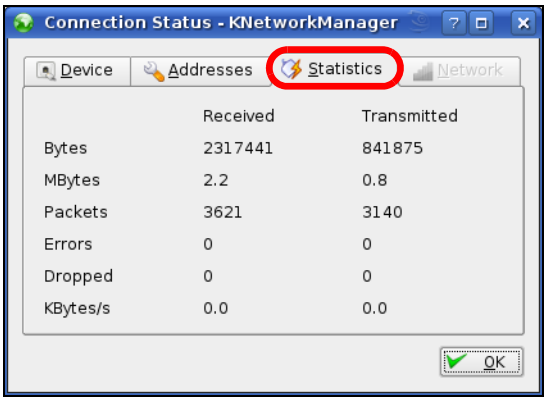


9 Click **Finish** to save your settings and close the window.

Verify the Settings

Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

When the **Connection Status** – **KNetwork Manager** window opens, click the **Statistics** tab to check if your connection is working properly.


Connection Status - KNetworkManager
Device
Addresses
Statistics
Network
Received
Transmitted
Bytes
2317441
841875
MBytes
2.2
0.8
Packets
3621
3140
Errors
0
0
Dropped
0
0
KBytes/s
0.0
0.0
OK

APPENDIX C
Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 53 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.

Table 53 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
STRM WORKS	UDP	1558	Stream Works Protocol.

Table 53 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

APPENDIX D
Legal Information

Copyright

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

UNITED STATES of AMERICA

The following information applies if you use the product within USA area.

US Importer: Zyxel Communications, Inc, 1130 North Miller Street Anaheim, CA92806-2001, https://www.zyxel.com/us/en/

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

EUROPEAN UNION and UNITED KINGDOM

The following information applies if you use the product within the European Union and United Kingdom.

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED) and UK regulation

- Compliance information for wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:
  - the band 2,400 to 2,483.5 MHz is 99.54 mW,
  - the bands 5,150 MHz to 5,350 MHz is 175.79 mW,
  - the 5,470 MHz to 5,725 MHz is 874.98 mW.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС. **National Restrictions** • The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. • Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. • Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE..
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. **National Restrictions** • In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.

Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. **National Restrictions** • This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details. • Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. **National Restrictions** • The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. • 2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU and United Kingdom market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC and UK regulation establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless settings, please refer to the chapter about wireless settings for more detail.)

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。

- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online at www.zyxel.com to receive email notices of firmware upgrades and related information

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: https://www.zyxel.com/form/gpl_oss_software_notice.shtml

Index

Numbers

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W